# 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」

経済産業省

２００２年４月

# はじめに

電子商取引の進展、電子政府の具体化に代表される、社会・経済のコンピュータ・ネットワーク利用の高度化の進展により、コンピュータ・システム上で処理されるデータ及びネットワーク上でやりとりが行われるデータの質・量は急速に深化・拡大している。

コンピュータ・システム及びそれによって処理されるデータのセキュリティの確保、すなわち秘密性、完全性、可用性の保護については、システム管理者、利用者の自己責任に基づく適切な組織的対応及び技術的対応体制の確立がまずもって行われる必要があるが、一方で、セキュリティを侵害する行為を禁圧するのに必要な処罰を与える刑事法制の整備及びこれを実質的に担保する刑事手続法制（以下、「サイバー刑事法制」という。）の整備も重要となる。

コンピュータ犯罪は、通常、対象が有体物ではなく情報であるが、情報はそれ自体としては可視性・可読性がないこと、作成主体をそれ自体から特定することが困難なこと、処理・加工が容易で犯罪の証跡が残りにくいといった特徴があり、さらにインターネットを始めとするネットワークを悪用する犯罪は、匿名性が高い、犯罪の痕跡が残りにくい、被害が同時に広範囲に及び得る、国境を超えることが容易であるいう特徴を有する。したがって、サイバー刑事法制は、かかる犯罪の特徴に対応したものである必要があり、ことに、インターネットのグローバル性に鑑みれば、実体法の内容について国際的な調和が必要であると当時に、手続法は、国際共助・協力が円滑に行われることを確保するものである必要がある。

我が国におけるコンピュータ関連犯罪に対応するために刑事法制の整備としては、昭和 62 年の刑法改正により、電磁的記録不正作出罪、電子計算機損壊等業務妨害罪、電子計算機使用詐欺罪、電磁的記録毀棄罪などが新たに設けられた。また、電気通信回線に接続している電子計算機に対する不正アクセス行為等を可罰化するための法整備としては、平成 11 年の不正アクセスの禁止等に関する法律の制定がこれまでも行われてきたところである。

他方、国際的には、G8 リヨングループ・ハイテク犯罪サブグループにおいて、特に Traceability（追跡可能性）の確保についての議論が熱心に行われてきており、また、欧州評議会では、1997 年以来、サイバー犯罪についての調査検討が進められ、昨年 11 月 8 日の欧州評議会閣僚委員会会合で、「サイバー犯罪に関する条約」が正式に採択され、同月 23 日に開催された署名式典で各国に開放された。欧州評議会加盟国、米国、カナダ等と並んで、我が国も同日、同条約に署名した。本条約は、サイバー犯罪からの社会の保護を目的とする国際的な法的枠組みを定めるものであり、サイバー犯罪の深化・蔓延に効果的かつ迅速に対処するために国際協力を行い、共通の刑事政策を採択することを目指している。具体的には、コンピュータ・システムへの不正なアクセス、不正な傍受等一定の行為を犯罪とすることを締約国に義務づけた上で、これらの一定の犯罪についての裁判権の設定、これらの一定の犯罪及びコンピュータ・システムという手段によって行われる他の犯罪についての犯罪人引き渡し並びに捜査、訴追及び司法手続における法律上の援助等について規定している。

本条約は、サイバー犯罪対策分野における世界初の条約であり、我が国もこれに署名したことを踏まえれば、本条約を基に、我が国のサイバー刑事法制のあり方を検討し、条約を批准するとした場合に必要となる立法作業及び検討が必要な論点について十分な検討を行うことは、政府内部のみならず、我が国全体にとっての喫緊の課題と言える。特に、その際には、可罰的行為の適切な処罰や、捜査手続の迅速・円滑な実施のみならず、個人情報・プライバシーの保護や、民間事業者への過重なコスト負担の回避という観点も踏まえた上で、国際的にも調和のとれた、バランスのとれた法制度の整備を目指す必要がある。

そこで、本サイバー刑事法研究会では、本条約の内容及び我が国に与えるインパクトについて正確に理解するために、条約の内容を精査し、かつ現行の刑事法制を前提として、条約上の義務が担保されていない又は担保されていない可能性が高いと考えられる条項について、これを担保するために必要な立法措置についての試案及び検討の方向性、検討すべき論点の整理を提示することとしたものである。加えて、検討の際に参考となる、各国の刑事法制の調査も行った。

本報告書が、我が国における、サイバー刑事法制に関する建設的な議論に資するものとなれば幸いである。

＜サイバー刑事法研究会 構成員＞

| | | |
|---|---|---|
| 〔座　長〕 | 山　口　　厚 | 東京大学大学院法学政治学研究科教授（刑法） |
| | 井　窪　保　彦 | 阿部・井窪・片山法律事務所弁護士 |
| | 歌　代　和　正 | インターネット・イニシアチブ・ジャパン株式会社<br>システム技術部部長 |
| | 佐　伯　仁　志 | 東京大学大学院法学政治学研究科教授（刑法） |
| | 酒　巻　　匡 | 上智大学法学部教授（刑事訴訟法） |
| | 中　原　志　郎 | 日本電信電話株式会社<br>第五部門担当部長 |
| | 夏　井　高　人 | 明治大学法学部教授（法情報学） |
| | 松　尾　正　浩 | 株式会社三菱総合研究所<br>ビジネスソリューション事業本部主任研究員 |
| | 丸　橋　　透 | 富士通株式会社　法務・知的財産権本部<br>法務部法務企画部担当課長 |
| | 村　島　俊　宏 | 村島・穂積法律事務所弁護士 |

（敬称略、50 音順）

＜サイバー刑事法研究会　オブザーバ＞

| | | | |
|---|---|---|---|
| 経済産業省 | 大　野　秀　敏 | 商務情報政策局 | 情報セキュリティ政策室室長 |
| 経済産業省 | 早　貸　淳　子 | 商務情報政策局 | 情報経済課課長補佐（2001 年 8 月まで） |
| 経済産業省 | 西　江　昭　博 | 商務情報政策局 | 情報経済課課長補佐 |
| 経済産業省 | 久　米　　孝 | 商務情報政策局 | 情報セキュリティ政策室　課長補佐 |
| 経済産業省 | 山　本　文　土 | 商務情報政策局 | 情報セキュリティ政策室　課長補佐 |
| 経済産業省 | 山　下　隆　也 | 経済産業政策局 | 知的財産政策室　課長補佐 |
| 経済産業省 | 服　部　　誠 | 経済産業政策局 | 知的財産政策室　課長補佐 |

# 目　次


**1.** サイバー犯罪条約逐条解説 ..... 1

**1.1.** 第 1 条　定義（Definitions） ..... 5

**1.2.** 第 2 条　不正アクセス（Illegal access） ..... 7

**1.3.** 第 3 条　不正な傍受（Illegal interception） ..... 10

**1.4.** 第 4 条　データの妨害（Data interference） ..... 13

**1.5.** 第 5 条　システムの妨害（System interference） ..... 15

**1.6.** 第 6 条　装置の濫用（Misuse of devices） ..... 17

**1.7.** 第 7 条　コンピュータに関連する偽造（Computer-related forgery） ..... 22

**1.8.** 第 8 条　コンピュータに関連する詐欺（Computer-related fraud） ..... 24

**1.9.** 第 9 条　児童ポルノに関連する犯罪（Offences related to child pornography） ..... 26

**1.10.** 第 10 条　著作権及び関連する権利の侵害に関する犯罪 ..... 29

**1.11.** 第 11 条　未遂及びほう助又は教唆（Attempt and aiding or abetting） ..... 31

**1.12.** 第 12 条　法人の責任（Corporate liability） ..... 33

**1.13.** 第 13 条　制裁及び措置（Sanctions and measures） ..... 35

**1.14.** 第 14 条　手続規定の適用範囲（Scope of procedural provisions） ..... 36

**1.15.** 第 15 条　条件及び保障条項（Conditions and safeguards） ..... 38

**1.16.** 第 16 条　蔵置されたコンピュータ・データの迅速な保全 ..... 40

**1.17.** 第 17 条　通信記録の迅速な保全及び部分開示 ..... 44

**1.18.** 第 18 条　提出命令（Production order） ..... 46

**1.19.** 第 19 条　蔵置されたコンピュータ・データの捜索及び押収 ..... 49

**1.20.** 第 20 条　通信記録のリアルタイム収集（Real-time collection of traffic data） ..... 54

**1.21.** 第 21 条　通信内容の傍受（Interception of content data） ..... 58

**1.22.** 第 22 条　裁判権（Jurisdiction） ..... 60

**1.23.** 第 23 条　国際協力に関する一般原則 ..... 63

**1.24.** 第 24 条　犯罪人引渡し（Extradition） ..... 64

**1.25.** 第 25 条　相互援助に関する一般原則 ..... 67

**1.26.** 第 26 条　自発的な情報提供（Spontaneous information） ..... 69

**1.27.** 第 27 条　適用可能な国際協定が存在しない場合の相互援助の要請に関する手続 ..... 71

**1.28.** 第 28 条　秘密性及び使用制限（Confidentiality and limitation on use） ..... 75

**1.29.** 第 29 条　蔵置されたコンピュータ・データの迅速な保全 ..... 77

**1.30.** 第 30 条　保全された通信記録の迅速な開示 ..... 80

**1.31.** 第 31 条　蔵置されたコンピュータ・データへのアクセスに関する相互援助 ..... 82

**1.32.** 第 32 条　同意に基づく又は公的に利用可能な蔵置されたコンピュータ・データへの国境を越えるアクセス ..... 84

**1.33.** 第 33 条　通信記録のリアルタイム収集に関する相互援助 ..... 85

**1.34.** 第 34 条　通信内容の傍受に関する相互援助 ..... 86
**1.35.** 第 35 条　二十四/七ネットワーク（24/7 Network） ..... 87
**2.** 現行法で担保されていない条項の担保の方法についての試案 ..... 89
**2.1.** 実体法 ..... 89
**2.2.** 手続法 ..... 90
**3.** 各国法制度の現状 ..... 94
**3.1.** 刑事実体法に係わる各国法制度の現状 ..... 94
**3.2.** 刑事手続法に係わる各国法制度の現状 ..... 112

参考文献

「海外サイバー犯罪関連法の動向調査に関する報告資料」

## 1. サイバー犯罪条約逐条解説

サイバー犯罪条約は、第 1 章から第 4 章までの 4 つの章、48 の条文で構成されている。第 1 章ではサイバー犯罪に関する基本用語を定義している。第 2 章では、刑事実体法として「不正アクセス」「不正傍受」「データ妨害」「システム妨害」「装置濫用」「コンピュータ関連偽造」「コンピュータ関連詐欺」「児童ポルノ関連犯罪」「著作権及び関連諸権利の侵害に関連する犯罪」をサイバー犯罪として定義し、構成要件を規定するとともに、コンピュータ・データの応急保全や部分開示、捜索・押収、通信記録（トラフィック・データ）のリアルタイム収集や通信内容の傍受などに関する手続法を定めている。第 3 章は第 2 章で定義したサイバー犯罪についての相互援助および引渡し命令を含む国際協力について規定している。第 4 章では最終条項として、欧州評議会条約の標準規定について述べている。ここでは、第 4 章の最終条項を除く、第 1 条から第 35 条までの各逐条について解説する。

本報告書における逐条の和訳は、外務省作成の仮訳を使用している。条約で使用されている重要な用語、原文において意味が明確でない、あるいは和訳と原文との間に意味の差違があるなど、研究会で議論の対象となった用語については、その定義を表１－1に示す。

逐条解説の部分については、参照した EM（Explanatory Memorandum Related Thereto）番号を示した。詳細については、該当する EM を参照のこと。

各逐条毎の「研究会における意見」は、本研究会において様々な議論がなされたことを示したものであり、記述内容の中には研究会の総意でないものも含まれている。また、報告書の性質上、明示していない場合であっても、複数の意見を併記している場合がある。

**表 1-1　サイバー犯罪条約　用語一覧（1/3）**

| 該当条文 | オリジナル | 外務省仮訳 | 条約中の定義　／　研究会での意見 |
|---|---|---|---|
| 第 1 条 | computer system | コンピュータ・システム | 何らかの装置又は相互に接続され若しくは関連する装置の一群であって、その中の一又は二以上の装置がプログラムに従ってデータの自動処理を行うもの |
| 第 1 条 | computer data | コンピュータ・データ | コンピュータ・システムにおける処理に適した形式による事実、情報又は概念の表象。コンピュータ・システムに機能を実行させるのに適したプログラムを含む。 |
| 第 1 条 | service provider | サービス・プロバイダ | (ⅰ)そのサービスの利用者に対してコンピュータ・システムという手段によって通信する能力を提供する公的又は私的な団体<br>(ⅱ)ⅰに規定する通信サービス又はその利用者のために、コンピュータ・データを処理又は蓄積するその他の団体 |
| 第 1 条 | traffic data | 通信記録 | コンピュータ・システムという手段による通信に関するコンピュータ・データであって、通信の連鎖の一部を構成するコンピュータ・システムによって作り出され、かつ、その通信の発信元、あて先、経路、時刻、日付、大きさ、持続時間又はその背後にあるサービスの種類を示すもの |
| 第 2 条等 | intentionally | 故意に | wilfully と区別して「意図して」との訳が好ましいとの意見もあるが、条約において使い分けに意味があるか否かについては、ドイツ語訳等も参考にして検討する必要がある。 |
| 第 2 条等 | security measures | 安全措置 | 不正アクセス禁止法における「アクセス制御機能」と同意と解釈することが可能である。 |
| 第 2 条 | access | アクセス | コンピュータ・システム（ハードウェア、コンポーネント、システム上に蔵置されたデータ、ディレクトリ、通信記録およ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（EM46） |
| 第 2 条 | illegal access | 不正アクセス | コンピュータ・システムおよびコンピュータ・データのセキュリティ（機密性、完全性及び可用性）に対して甚大な被害をもたらす、またはこれに対して攻撃をする基本的な犯罪行為（EM44）。<br>「違法アクセス」との訳が好ましいのではないか。<br>不正アクセス禁止法の一般的な和訳によれば、「不正アクセス」は、「unauthorized access」となっている。 |
| 第 3 条 | illegal interception | 不正な傍受 | 「違法傍受」との訳が好ましいのではないか。<br>同上 |

**表１－１　サイバー犯罪条約　用語一覧（2/3）**

| 該当条文 | オリジナル | 外務省仮訳 | 条約中の定義　／　研究会での意見 |
|---|---|---|---|
| 第 3 条 | non-public transmission | 非公開送信 | 当事者が秘扱いの形態で通信しようとしている送信、サービスに対する対価の支払いがあるまでは商業目的上秘密が保たれる送信といったものも含まれ、公共ネットワークを介した送信を排除するものではない（EM54）。 |
| 第 5 条 | Hindering | 妨害 | コンピュータ・システムの本来の機能に干渉する行為（EM66） |
| 第 6 条 | Distribution | 頒布 | 他人にデータを転送する能動的な行為。オンライン・デバイスへのアクセスを助長するハイパーリンクの作成や編集を含む（EM72）。 |
| 第 6 条 | making available | 利用可能とする | 他人の使用のためにオンライン・デバイスを他人の用に供すること（EM72） |
| 第 8 条 | fraud | 詐欺 | 条約における「fraud」は、日本語の「詐欺」ということばよりも意味する範囲が広く、日本においては「窃盗」にあたる犯罪も含むと考えられる。 |
| 第 8 条 | loss of property | 財産上の損害 | 金銭の損害、有形・無形の経済的価値の損害を含む（EM88）。 |
| 第 10 条 | wilfully | 故意に | 知的財産権の条約で使用されている用語のため第 10 条の著作権侵害罪についてのみ使用されている。Intentionally と区別して「意欲して」との訳が好ましいとの意見もあるが、条約においてなされている使い分けに意味があるか否かについては、ドイツ語訳等も参考にして検討する必要がある。 |
| 第 12 条 | civil liability | 民事責任 | 条約においては civil penalty のようなものを想定しており、日本における損害賠償を sanction の一種であると解釈することには疑問があるとの意見もある。 |
| 第 13 条 | effective | 効果的な | 「効果的な」ということばが、「自由の剥奪」を常に要求するか否かという解釈の問題がある。 |
| 第 13 条 | dissuasive | 抑止力のある | 「抑止力のある」ということばが、「自由の剥奪」を常に要求するか否かという解釈の問題がある。 |
| 第 16 条等 | stored | 蔵置された | 「蔵置」は、税関係の法令において、課税物件を倉庫、貯蔵所等にしまい貯めておくことをいうと解するのが通例のようであるが、本条においては、そのような特別の意味はないことから、「保存」「記憶」等と訳した方が適切ではないか。 |
| 第 16 条等 | preservation | 保全 | 既にコンピュータ・データとして存在しているデータが、改変、劣化および削除から保護されていること（一定のデータの収集や保存を義務づけるものではない）（EM152）。 |

**表１－１　サイバー犯罪条約　用語一覧（3/3）**

| 該当条文 | オリジナル | 外務省仮訳 | 条約中の定義　／　研究会での意見 |
|---|---|---|---|
| 第 18 条 | subscriber information | 加入者情報 | サービス・プロバイダによって保有されるサービス加入者に関連する情報のうち、トラフィック・データ及びコンテント・データ以外のコンピュータ・データその他の情報であって、それにより次のことが立証されるもの。<br>(a) 使用された通信サービスの種類、そのために使用された技術的設備及びサービスの期間<br>(b) サービス契約又は取極に基づいて利用可能な加入者の特定、郵便上の又は地理的な住所、電話番号その他のアクセスのための番号並びに請求及び支払に関する情報<br>(c) サービス契約又は取極に基づいて利用可能な通信機器の設置場所に関する情報その他の情報 |
| 第 19 条 | search | 捜索 | データを探索、閲読、検査、調査すること。これは、データの捜索と、（調査する）データの探索という意味を含んでいる（EM191）。 |
| 第 19 条 | seizure | 押収 | データもしくは情報が記録された物理媒体を取り上げること、またはデータもしくは情報の複製を作成して保持すること。押収されるデータの使用又はそれにアクセスするのに必要なプログラムの押収も意味している（EM197）。 |
| 第 21 条 | content data | 通信内容 | 通信上の通信内容。例えば、通信の意味または意図、通信によって伝達される（通信記録以外の）メッセージまたは情報である（EM209, 229）。 |

## 1.1. 第 1 条　定義（Definitions）

(1) 逐条

【原文】

For the purposes of this Convention:

a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*;*

c. “service provider” means:

(i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

(ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d. “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

【和訳】

この条約の適用上、

(a) 「コンピュータ・システム」とは、何らかの装置又は相互に接続され若しくは関連する装置の一群であって、その中の一又は二以上の装置がプログラムに従ってデータの自動処理を行うものをいう。

(b) 「コンピュータ・データ」とは、コンピュータ・システムにおける処理に適した形式による事実、情報又は概念の表象をいい、コンピュータ・システムに機能を実行させるのに適したプログラムを含む。

(c) 「サービス・プロバイダ」とは、次のものをいう。

(ⅰ) そのサービスの利用者に対してコンピュータ･システムという手段によって通信する能力を提供する公的又は私的な団体

(ⅱ) ⅰに規定する通信サービス又はその利用者のために、コンピュータ・データを処理又は蓄積するその他の団体

(d) 「通信記録」とは、コンピュータ・システムという手段による通信に関するコンピュータ・データであって、通信の連鎖の一部を構成するコンピュータ･システムによって作り出され、かつ、その通信の発信元、あて先、経路、時刻、日付、大きさ、持続時間又はその背後にあるサービスの種類を示すものをいう。

(2) 逐条解説

本条は犯罪条約における「コンピュータ・システム」、「コンピュータ・データ」、「サービス・プロバイダ」、「通信記録」の 4 つの概念について定めるものである。各締約国の国内法においてこれらの概念を逐語的に使用する義務はないが、条約加盟にあたっては条約の基本原則と一致するような方法によりこれらの概念をカバーする必要がある。

「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およびソフトウェアで構成される装置であり、スタンドアロンのものとネットワーク接続されたもののいずれでもありうる。ここでいうネットワークとは 2 つ以上のコンピュータ・システムの相互接続であり、その接続方法についてはケーブル、無線電話、赤外線、通信衛星の別を問わない（EM23－24）。

「コンピュータ・データ」は ISO のデータ定義に基づいており、コンピュータ・システムによって直接処理可能な形式のデータである (EM25。)

「サービス・プロバイダ」は、コンピュータ・システム上でのデータ通信またはデータ処理に関する特別の役割を果たすという広範なカテゴリーを包含しており、利用者に代わりデータを記憶し、その処理を行うような主体も含んでいる (EM26－27) 。

「通信記録」は、特定の法領域の対象となるコンピュータ・データについての区分されたカテゴリーであり、犯罪条約中で特定の領域として取り扱われるカテゴリーを本条により限定列挙している（EM28－31）。

(3) 研究会における意見

HTTP という抽象化された通信路形態の出現により通信手段の多様化が進んできており、「コンテント・データ」（EM229）と「通信記録」の区分（EM209）が困難なケースが今後増えていくものと予想される。特に手続法における保全、捜索・押収、リアルタイム収集等の条項においてこの点が議論となる。

## 1.2.第 2 条　不正アクセス（Illegal access）

(1) 逐条

【原文】

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

【和訳】

締約国は、自国の国内法により、コンピュータ・システムの全部又は一部に対するアクセスが、権限なしに故意に行われることを犯罪とするため、必要な立法その他の措置をとる。締約国は、当該アクセスが安全措置を侵害することによって行われること、コンピュータ・データを入手する意図その他不誠実な意図をもって行われること又は他のコンピュータ・システムに接続されているコンピュータ・システムに関連して行われることをこの犯罪の要件とすることができる。

(2) 逐条解説

本条は、コンピュータ・システムへの違法アクセスについて定めたものである。ここでいう「アクセス」とは、コンピュータ・システムの全部または一部に入ることを意味する。ただし、システムへの電子メール・メッセージやファイルの単なる送信行為は含まれない。公共通信ネットワークを介して接続された他人のコンピュータ・システムや、ある組織内のＬＡＮやイントラネットのような同一のネットワーク上に存在する他のコンピュータ・システムに入ることが含まれており、通信手段の別は問題とならない（EM46)。

国内法では、「不正アクセス行為の禁止等に関する法律（以下「不正アクセス禁止法」という。）の規定が本条の規定に該当するが、同法第 3 条第 2 項の各号では不正アクセスの対象となるコンピュータは、「アクセス制御機能を有する特定電子計算機（電気通信回線に接続している電子計算機)」に限定されている。犯罪条約では、不正アクセスの対象は「コンピュータ・システムの全部又は一部」となっており、「アクセス制御機能を有する」、「電気通信回線に接続している」といった限定は付されていない。このため、本条の担保にあたっては、現行の不正アクセス禁止法において、「アクセス制御機能を有さないコンピュータ」や「電子通信回線に接続していない電子計算機」に対するアクセス行為が処罰の対象とならないという点が論点となる。ただし、本条では、「安全措置を侵害することによって行われること(infringing

security measures)」を要件とすることができるとされており、これを要件とすれば概ね「アクセス制御機能を有する」との要件が存在する場合と同様の結果が得られると解釈することが可能である。さらに「他のコンピュータ・システムに接続されているコンピュータ・システムに関連して行われること(in relation to a computer system that is connected to another computer system)」を要件とすることができるとされており、他のコンピュータを使用しないスタンドアロン・コンピュータへの物理的なアクセスという状況を排除することが許される。これを要件とすれば、概ね「特定電子計算機（電気通信回線に接続している電子計算機)」を要件とするのと同じ結果が得られると解釈することが可能である。

こうして、本条については、「安全措置を侵害することによって行われること」および「他のコンピュータ・システムに接続されているコンピュータ・システムに関連して行われること」の要件を付加することにより、国内法での担保が可能である。

(3) 研究会における意見

「他のコンピュータ・システムに接続されている」という要件については、これに対応する国内法におけるネットワーク（電気通信回線）の定義が確定されていないとの指摘があった。犯罪条約においては、「ネットワークに接続されたコンピュータ」に対する不法なアクセスのみを処罰対象とすることができること、及びそのネットワークは、通信サービスによって提供される公共ネットワーク及び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ことが明記されている（EM50)。これに対し、不正アクセス禁止法においては「電気通信回線」の定義が条文上はおかれていないが、その逐条解説によれば「電気通信を行うために設定される回線」をいい、「電気通信事業法上の電気通信回線設備の存在を前提に、論理的に設けられるものであって、有線、無線を問わない」と解釈されている

また、本条を現行国内法で担保するためには「他のコンピュータ・システムに接続されている」という要件を付加することが必要となるが、立法論として「他のコンピュータ・システムに接続されているコンピュータ・システムに関連して行われること」という要件がそもそも必要かどうか、つまり不正アクセスの対象に「スタンドアロン・コンピュータ」を含めるか否かという点については、重要なデータはスタンドアロン・コンピュータに格納されている場合も多いことから、これも処罰の対象とすべきとの意見も出される一方、仮にコンピュータ内の電磁的記録だけを対象に「アクセス制御侵害罪」的な構成要件を定立する場合、同じ「情報」でありながら、アナログの場合は刑法的保護の対象とならないものが、デジタルの場合は刑法的保護の対象となるということについて、既存の法制度との関係をどのように説明するのかという問題が生じるとの意見も出された。日本では、秘密侵害一般が刑法上処罰されないため、それと区別するためにネットワークに対するセキュリティを侵害するという点を捉えて、不正アクセス禁止法が現在のような形となったものであり、最初からスタンドアロンの不正アクセスを処罰できるということになれば、秘密の探知行為一般はどうな

るかという論点に波及し、日本の刑法体系の大きな変更が必要となるのではないかという問題になる。たしかに、スタンドアロン・コンピュータのアクセス制御侵害行為も、ネットワークに接続されたコンピュータに対するものと同様、処罰すべきであるとの意見も多いが、現行法においても、権限を有する者以外には立入りを許されていない場所に設置してあるスタンドアロン・コンピュータに対して、その設置場所に立入って物理的にアクセスした場合には、建造物侵入罪の処罰対象となるので、スタンドアロン・コンピュータのアクセス制御侵害を独立して処罰しなければならないような事案は、相当程度限定されるのではないかとの意見もあった。なお、デジタル情報とアナログ情報でアクセス制御機能の侵害の当罰性に違いが生じ得るかどうかについては、コンピュータ・チップに大量の情報が入っている場合、保護するのはコンピュータだからでなく、大量の情報が入っている蓋然性が高いからという説明が考えられるとの意見も出された。

不正アクセスまたは無権限アクセスは、データ妨害またはシステム妨害の手段行為又は予備行為である場合が多い。犯罪条約では不正アクセスそのものよりもその結果として生じるデータ妨害やシステム妨害を処罰することを主眼としている。その意味で、「他のコンピュータ・システムに接続されている」という要件を付加するときにはとくに、本条は予備的な行為を処罰する規定となるともいいうる。

無権限アクセスの成否については、米国の USC の第 1030 条の解釈論によると、現実にアクセス制御がなされていなくても、社会的観点から見てアクセス権があると評価できるかどうかによって、アクセス制御の有無を識別できるというのが米国の通常の考え方である。日本におけるアクセス制御の有無についての識別基準は不正アクセス禁止法第 3 条第 2 項に規定されているが、米国と比べると厳格なものとなっている。

## 1.3.第 3 条　不正な傍受（Illegal interception）

(1) 逐条

【原文】

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

【和訳】

締約国は、自国の国内法により、コンピュータ・システムへの若しくはそこからの又はその内部におけるコンピュータ・データの非公開送信（コンピュータ・データを運ぶコンピュータ・システムからの電磁的放射を含む。）に対する傍受が、技術的手段によって権限なしに故意に行われることを犯罪とするため、必要な立法その他の措置をとる。締約国は、当該傍受が不誠実な意図をもって行われること又は他のコンピュータ・システムに接続されているコンピュータ・システムに関連して行われることをこの犯罪の要件とすることができる。

(2) 逐条解説

本条は、コンピュータ・データの違法傍受について定めたものである。電話による会話に対する傍受および記録についての従来の規制と同様に、データ通信上のプライバシーに対する侵害からの保護を目的としている。本条における犯罪行為は、コンピュータ・データの「非公開送信」('non-public' transmissions)を対象とするものであり、電話、ファックス、電子メール、ファイル転送といった送信されるデータの形態の別は問題としていない（EM51）。ここでいう「非公開送信」とは、伝送（通信）プロセスの性質を規定するものではあるが、伝送されるデータの（内容の）性質を限定するものではない。「非公開送信」には、当事者が秘扱いの形態で通信しようとしている送信、サービスに対する対価の支払いがあるまでは商業目的上秘密が保たれる送信といったものも含まれ、公共ネットワークを介した送信を排除するものではない（EM54）。

国内法では、電気通信事業法（第 104 条第 1 項）および有線電気通信法（第 9 条、第 14 条第 1 項）により、電気通信事業者の取扱中に係る通信および有線電気通信については、秘密を犯す行為が処罰の対象とされているが、EM55 によれば、条約の対象には、１個のコン

ピュータ・システム内の伝送のように（例：CPU から画面又はプリンタへのフロー）、電気通信事業者の取扱中に係る通信及び有線電気通信には該当しないものも含まれると解されることから、国内法が犯罪条約で違法傍受の対象としているものの全てを処罰の対象としているとは言えない可能性もある。ただし、本条でも「他のコンピュータ・システムに接続されているコンピュータ・システムに関連して行われること」という要件を付加することができることになっており、それらのコンピュータ間での伝送が多くの場合、電気通信事業者の取扱中に係る通信又は有線電気通信に含まれると解することにより担保が可能と考えられる。

コンピュータ・システムの電磁的放射からのデータ傍受行為（いわゆる「テンペスト」）については、画面のみを傍受して解読する場合には処罰の対象とならないが、ケーブルから電磁的放射を傍受して解読する場合には、有線電気通信法の通信の秘密侵害罪により処罰の対象となると考えられる。

無線通信については、EM56 において「相対的に公開であり容易にアクセスできる手段」で行われる通信の傍受は処罰対象外とされているが、それ以外の通信の傍受については処罰対象としているとも反対解釈しうる。その場合、現行電波法においては、通信傍受行為のみでは処罰していない（電波法第 59 条により漏洩、窃用が構成要件となっている）ため、その整合性について検討が必要であり、現行電波法の改正が必要になる可能性がある。

(3) 研究会における意見

非公開送信(non-public transmissions)の定義については、「他のコンピュータ・システムに接続されているコンピュータ･システムに関連して行われること」の要件を付さない場合、スタンドアロン・コンピュータ内の送信も対象となる可能性があり、前条と同様の問題が生じる。

暗号化やスクランブルが施された非公開送信を契約者以外の者が傍受し復号化した場合、復号化する行為自体が不正傍受に該当するか否かについて解釈が明確になっていない。ドイツ刑法の解釈論では読めないデータを読めるようにすること自体を問題とする議論もある。また、傍受のみを行い復号化しなかった（できなかった）場合については、電波法では処罰対象となっていないが、電気通信事業法においては暗号が流れたことがわかるだけで通信の秘密の侵害に該当すると考えられており、整合性が取れているか否かについて検討が必要である。スクランブルのかかった無線通信については、無線通信自体は一般的には public であり傍受を行っても処罰の対象とならないが、スクランブルをはずす行為については本条における傍受として処罰の対象となるとの解釈も可能と考えられる。なお、通信を傍受して一旦ディスクに格納し格納したファイルを復号化する行為については、「傍受」に該当せず、あくまでも、傍受し復号化するという行為が一連のものとして行われた場合に、それが全体として「傍受」に該当しうるか否かという点が、ここでの問題であると考えられる。

テンペストについては、欧州におけるコンピュータセキュリティの考え方には electro magnetic emission の防止が含まれており、本条においても犯罪行為の対象に含まれるとさ

れているが、有線電気通信法の領域には対応する規定が存在しない。この点について、特に画面のみを傍受する場合、国内法で対応できているか明確でない部分がある。

### 1.4.第 4 条　データの妨害（Data interference）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

【和訳】

1. 締約国は、自国の国内法により、コンピュータ・データを権限なしに故意に破壊し、削除し、劣化させ、改ざんし又は隠ぺいすることを犯罪とするため、必要な立法その他の措置をとる。
2. 締約国は、１に規定する行為が重大な害を引き起こすことをこの犯罪の要件とする権利を留保すること　ができる。

(2) 逐条解説

本条は、記録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および正常な機能またはその使用について、意図的な加害行為からの保護を提供することを目的としており（EM60)、「権限なく」、「故意に」実行した場合のみを処罰の対象とする。ウィルスやトロイの木馬のような悪意あるコードを感染させる行為は、それがデータの改変に至る場合には、本条にいう「改ざん」に含まれる（EM61)。また、どのようなものが重大な危害を発生させることになるのかについての解釈は、締約国の国内法に任されているが、第２項に挙げる要件を付加する場合にはその解釈を通知することが義務付けられている（EM64)。

公務所の用に供する電磁的記録、権利又は義務に関する他人の電磁的記録の効用が害された場合、すなわち媒体の損壊や記録の消去がなされた場合には、当該電磁的記録について、刑法第 258 条および第 259 条の毀棄罪の規定を適用することにより、その刑法的保護を担保可能である。内容の消去、改変が新たな証明力を生じさせる場合は、電磁的記録不正作出（刑法第 161 条の 2）の問題となる。また、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に対する加害行為により、電子計算機の動作障害を生ぜしめ、その結果としてその人の業務を妨害した場合には、電子計算機損壊等業務妨害罪（刑法第 234 条の２）による担保が可能である。

コンピュータ・ウィルスをコンピュータ・データに感染させる行為については、当該デー

タの損壊などの実害が発生した場合には、電磁的記録毀棄罪（刑法第 258 条、第 259 条）等の適用により、その処罰を担保可能である。電磁的記録の損壊により、電子計算機の動作阻害が生じ、業務妨害の結果が発生した場合には、電子計算機損壊等業務妨害罪が成立し、実害が発生していない場合でも、駆除の必要を生ぜしめたことを理由に、業務妨害罪の適用の可能性がある。

第 2 項の留保（「行為が重大な害を引き起こすこと」）については、どのような行為が重大な害を引き起こすことになるかの解釈は各締約国に任される。したがって、留保を付する場合には、現行法で処罰の対象としている行為が、わが国の「重大な害を引き起こすこと」にあたるという説明をすることになる。

(3) 研究会における意見

公務所の用に供する電磁的記録、権利又は義務に関する他人の電磁的記録以外の電磁的記録については、その記録媒体が器物損壊罪の客体となり、同罪でいう「損壊」は物理的損壊に限らず、物の効用を害する一切の行為をいうが、実務的には、重要なファイルについての改ざん、損壊により大きな損害が出た場合のみが対象となると考えられる。また、電子計算機損壊等業務妨害罪や業務妨害罪の対象となる「業務」は、職業その他社会生活上の地位に基づき継続して行う事務又は事業をいい、娯楽として行う行為や日常の家庭生活は除外されると解されており、本条を担保するために欠けている部分があることは否定できないものの、実際上当罰的な場面はカバーされていると言え、それ以外の部分については、EM37 でいう「軽微又は些細な違反行為（petty or insignificant misconduct）」として処罰の対象から除外するとの解釈が可能である。

### 1.5.第 5 条　システムの妨害（System interference）

(1) 逐条

【原文】

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

【和訳】

締約国は、自国の国内法により、コンピュータ・データの入力、送信、破壊、削除、劣化、改ざん又は隠ぺいが権限なしに故意に行われ、コンピュータ・システムの機能に重大な妨害が行われることを犯罪とするため、必要な立法その他の措置をとる。

(2) 逐条解説

本条は、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することを意図的に妨害する行為を犯罪行為として処罰することを目的としており、「権限なく」、「故意に」実行した場合のみを処罰の対象とする。したがってコンピュータ・システムの保有者または運営者によって権限を与えられてなされる行為が「重大な妨害」という結果を発生させた場合は、処罰の対象とはならない（EM68）。また、「重大な妨害」とされるものの基準、妨害の客体となるシステムの機能の範囲・程度（部分か全体か、一時的か永続的か）、および国内法による制裁を行政罰とするか刑事罰とするかの制度設計は、締約国の判断に任せられている（EM67,69）。

国内法では「人の業務」を妨害することが処罰の要件とされているが、ここでいう「人の業務」とは「自然人、法人その他の団体が『職業その他社会生活上の地位に基づき継続して行う事務または事業』（大判大正 10・10・24 刑録 27 輯 643 頁）」と解釈されており、本条でいう「重大な妨害」が行われた場合は概ね「人の業務」が妨害された場合に該当すると思われる。また、説明用覚書によれば、本条の「重大な妨害」の基準は各締約国の決定に任されているため、わが国における「重大な妨害」の基準を明確に宣言することにより、刑法第 234 条の 2（電子計算機損壊等業務妨害）および刑法第 233 条（信用毀損及び業務妨害）、刑法第 234 条（威力業務妨害）による担保が可能である。

DDos 攻撃については、「大量に送付することは『不正な指令』である」との解釈をすれば、電子計算機損壊等業務妨害罪の適用により担保可能である。また、機械に対する対物的加害行為も「偽計」ないし「威力」に当たると解されることから、偽計業務妨害罪ないし威力業

務妨害罪の適用も考えられる。

(3) 研究会における意見

DDos 攻撃については、CPU の視点からみると正当な指令の送付であり、電子計算機損壊等業務妨害罪（刑法第 234 条の 2）が成立するか否かについて議論のあるところである。この点、大量に送るということは「不正な指令」を与えたことに該当するという解釈を採用するときには、DDos 攻撃も同条の処罰対象となりうる。ただし、刑法第 234 条の 2 における「不正な指令」の定義が現状では明確化されていないという問題があり、処罰範囲の弛緩を防ぐためには、偽計業務妨害罪（刑法第 233 条）の適用が望ましいとの意見もある。なお、電磁的なものによって物理的なものを攻撃する威力があると考えれば、威力業務妨害罪（刑法第 234 条）の適用も不可能ではない。

## 1.6.第 6 条　装置の濫用（Misuse of devices）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
   (a) the production, sale, procurement for use, import, distribution or otherwise making available of:
      (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
      (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

   with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
   (b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.
3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

【和訳】

１．　締約国は、自国の国内法により、権限なしに故意に行われる次の行為を犯罪とするため、必要な立法その他の措置をとる。
   (ａ) 第二条から前条までの規定に従って定められる犯罪を行うために使用する意図をもって、次のものを製造し、販売し、使用のために調達し、輸入し、配布し又はその他の方法によって利用可能とすること。
      (ｉ) 第二条から前条までの規定に従って定められる犯罪を主として行うため設

計され又は調整された装置(コンピュータ・プログラムを含む。)

(ii) コンピュータ･システムの全部又は一部にアクセス可能となるようなコンピュータ・パスワード、アクセス・コードその他これらに類するデータ

(b) 第二条から前条までの規定に従って定める犯罪を行うために使用する意図をもって、ａｉ又はiiに規定するものを保有すること。締約国は、自国の法令により、これらのものの一定数の所持を刑事責任が生ずる要件とすることができる。

2. この条の規定は、１に規定する製造、販売、使用のための調達、輸入、配布若しくはその他の方法によって利用可能とする行為又は保有が、コンピュータ・システムの正当な試験又は保護等第二条から前条までの規定に従って定められる犯罪を行うことを目的としない場合には、刑事責任を課するものと解してはならない。

3. 締約国は、留保が１ａiiに規定するものを販売、配布又はその他の方法によって利用可能とする行為に関するものでない場合には、１の規定を適用しない権利を留保することができる。

(2) 逐条解説

本条は、犯罪条約第 2 条～第 5 条に規定する犯罪を実行する意図で特定の装置（ソフトウェアを含む）あるいはデータの製造・販売等の行為を、第 2 条～第 5 条とは独立した犯罪として処罰することを目的としている。

本条の第 1 項（a）(i)においては、ハッキングツール等の不正プログラムやコンピュータ・ウィルスについて、（a）(ii)においては、コンピュータ・システムの全部又は一部へのアクセスを可能とするコンピュータ・パスワード、アクセス・コードまたはこれらに類するデータについて、製造、販売、使用のための調達、輸入、配布またはその他の方法によって利用可能にする行為を犯罪として処罰することを規定している。「配布」とは、他人にデータを転送する能動的な行為を指すのに対し、「利用を可能とする」とは、オンライン・デバイス（通常はソフトウェアと考えられる）を他人の用に供することをいい、そのようなデバイスへのアクセスを助長するハイパーリンクの作成等をカバーする意図である（EM72)。起草段階で、処罰対象となるデバイスを専ら犯罪実行の目的で設計されたものに限定するか、いわゆる”dual-use devices”を除外すべきかどうかについて相当な議論があったが、そのように限定するとあまりに処罰対象が狭すぎて実際の刑事手続では適用不能になると考えられ、他方、適法に製造・配布されている場合も、全てのデバイスを含ませるという案も拒否された。合理的な妥協案として、主として犯罪実行の目的で客観的に設計されている場合に限定することとしている（EM73)。また、第 1 項ｂにおいて、第 2 条～第 5 条に規定する犯罪を行うために使用する意図をもってする、これらの物件の保有行為についても処罰の対象としている。なお、解釈宣言により、一定数以上の物を所持することを犯罪成立要件とすることが認められ、かつその数の決定は締約国に任されている。また、第 2 項において、コンピュータ・システムの正当な試験または保護等、犯罪を目的としない場合には、本条の対象としないこと

が規定されている（EM77）。

第１項(a)(ⅰ)については、不正プログラム、コンピュータ・ウィルス等を用いて実際にコンピュータのシステムダウンやプログラムの破壊等の結果を生じさせた場合には、国内法においても刑法第 234 条の 2（電子計算機損壊等業務妨害罪）などで処罰されるが、かかる結果を生じさせる意図を持って行われる不正プログラムの製造・頒布行為についての規制が我が国には存在しないので、本条項は現在の国内法では担保されていない。ただし、第 3 項による留保をつけることが可能であるので、留保すれば国内法を改正する必要はない。

第１項（a）(ii)は、条約第 2 条から第 5 条に規定する犯罪、すなわち我が国においては、不正アクセス禁止法上の不正アクセス行為、電気通信事業法及び有線電気通信法等の「通信の秘密」侵害行為、刑法上の電磁的記録毀棄罪、電子計算機損壊等業務妨害罪等の実行行為を行うために使用する意図をもって、コンピュータ・システムの全部又は一部へのアクセスを可能とするパスワード、アクセス・コード等のデータを製造、販売、使用のための調達、輸入、配布又はその他の方法によって利用可能とする行為を処罰するものである。我が国においては、不正アクセス禁止法第４条において「アクセス制御機能に係る他人の識別符号を、その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして、又はこれを知っている者の求めに応じて」無権限者に提供することが禁じられている。本条約が規定するような場合には、「その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして、又はこれを知っている者の求めに応じて、」なされることがほとんどであると思われ、この論点に関しては、客体となるコンピュータが電気通信回線に接続されていれば、本条約が処罰の対象とする行為のほとんどが不正アクセス禁止法による処罰の対象となっている可能性がある。しかしながら、不正アクセス禁止法では「特定電子計算機（電気通信回線に接続されている電子計算機）の特定利用（電気通信回線を通じて行うもの）に係るもの」であることが要件となっているので、スタンドアロン・コンピュータを客体とする犯罪に使用する意図しかない場合には、同法の適用は困難となる。条約第 2 条（不正アクセス）と第 3 条（不正な傍受）においては、解釈宣言を付せば、電気通信回線に接続されている電子計算機を対象とする行為のみを処罰の対象とすることができるが、第 4 条（データの妨害）および第 5 条（システムの妨害）ではそのような要件が付すことができない。すなわち、スタンドアロン・コンピュータを対象とするシステム妨害・データ妨害に使用する意図で、パスワード等を提供する行為については、現行のままでは国内法での担保がなされていない。

(3) 研究会における意見

第 6 条(a)(ii)については、不正アクセス禁止法第 4 条（不正アクセス行為を助長する行為の禁止）にあたるものであれば、スタンドアロン・コンピュータが客体となる場合を除いて、

大部分が同条の適用により担保可能である。スタンドアロン・コンピュータを客体とするパスワードの違法複製について、米国においては、無権限アクセスの一類型とされているが、わが国においては、直接該当する犯罪類型はないと考えられる。

第 4 条、第 5 条との関連におけるスタンドアロン・コンピュータの扱いについては、各条に対する予備罪的な規定を設けて対応することも考えられるが、国内法で予備罪が設けられている犯罪類型は極めて重大な犯罪類型に限られており、予備罪の設けられていない他の犯罪類型との均衡について考慮する必要がある。他方、新たな犯罪類型の創設については、最近行われた支払用カードの偽造等の犯罪に対処するための刑法改正の例が参考になると思われる。同罪は、事務処理の用に供する電磁的記録であって、クレジットカード等を構成するものを不正に作った者を処罰しているが、今次の改正で、当該犯罪の用に供する目的で、当該電磁的記録の情報を取得した者、情を知って当該犯罪の用に供する電磁的記録の情報を提供した者を処罰することとしたものである（刑法第 163 条の 4 等)。もっとも、同罪の対象となる電磁的記録の情報は、「カードを構成する電磁的記録」として一義的に特定することが困難ではないが、「電磁的記録損壊」や「電子計算機損壊等業務妨害罪」を犯す目的で、①コンピュータ・パスワード等のデータや、②コンピュータ・ウィルス等のプログラムを作る行為を罰するとした場合、客体及び行為態様の明確化がどこまで具体的に行えるかがポイントとなる。①の場合は当該データを有する権限を有する者と有しない者を区別することは比較的容易と考えられるので、客観的な状況から立件を行うことも比較的容易と考えられるが、②の場合は処罰の客体となるプログラムとならないプログラムを客観的に区別することは容易でないと考えられる。したがって、立法技術的にはパスワードの所持自体を可罰化することの方が、一定のプログラムを保持することを可罰化するよりも困難は少ないと考えられるが（軽犯罪法第 1 条第 3 号参照〔「正当な理由がなくて合いかぎ、のみ、ガラス切りその他他人の邸宅又は建物に侵入するのに使用されるような器具を隠して携帯していた者」を拘留又は科料に処する〕)、デジタル情報の「アクセス制御」を行うパスワードを処罰対象とし、アナログ情報についての「アクセス制御」を行う、例えば、金庫の鍵の保有等を処罰対象としないとすれば、情報の形態がデジタルか、アナログかによってその刑法的保護の態様が変わることになり、その点について合理的な説明が可能か否かが問題となる。

以上のいずれの場合であっても、新たな犯罪類型を刑法典の中に含めるか否かも含めた検討が必要であるが、サイバー刑事法制に関連する規定は、なるべく包括的に、わかりやすい形式で規定すべきと考えられる。

また、不正アクセス禁止法の改正で対応することは、「電気通信回線を通じて」行われる電子計算機に係る犯罪の防止とアクセス制御機能により実現される「電気通信に関する秩序の維持」という同法の目的を改正することが必要になると考えられ、抜本的な改正が必要となると考えられる。また、仮にコンピュータ内の電磁的記録だけを対象に「電気通信回線に関する秩序」と切り離して「アクセス制御侵害罪」的な構成要件を定立する場合、上述のとおり、同じ「情報」でありながら、アナログの場合は刑法的保護の対象とならないものが、デ

ジタルの場合は刑法的保護の対象となるということについて、既存の法制度との関係をどのように説明するのかという問題が生じる。

第 6 条(a)（ⅰ)に規定する犯罪使用目的による不正プログラムの製造・頒布等の処罰化については、留保が可能であるため、新たな立法化をせずとも条約への加盟は可能であるが、仮に当該行為を処罰するとすれば、産業界、とりわけ情報セキュリティ関係企業、研究機関等への影響も大きいと考えられる。「不正」な結果を発生させ得るプログラムであっても、正当な業務目的でも利用される場面が考えられるため、プログラムの客観的な性質だけで「不正」か否かを決することは難しく、理論的には、プログラムの客観的な性質に加えて、犯罪を行うために使用する意図の有無により処罰の対象となるか否かを判断するという判断枠組みが必要となると考えられる。もっとも実際上は、結果が発生して初めて目的の存在が確認される場合が多くなると思われる。正当な業務目的、研究目的で用いられ得るセキュリティ監査ツールなども、犯罪目的がある場合にはその所持について処罰の対象となる可能性が生じるため、仮に、以上のような処罰規定を新たに設ける場合であっても、自由なプログラム開発やビジネスに抑制効果が生じないよう、構成要件の明確性については十分な検討が必要である。

## 1.7.第 7 条　コンピュータに関連する偽造（Computer-related forgery）

(1) 逐条

【原文】

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

【和訳】

締約国は、自国の国内法により、コンピュータ・データ（直接読取可能であるかないか及び理解可能であるかないかを問わない。）が法律上の目的において真正であるとみなされ又は扱われる意図をもって、コンピュータ・データを権限なしに故意に入力し、改ざんし、削除し又は隠ぺいし、その結果として真正でないデータを生じさせる行為を犯罪とするため、必要な立法その他の措置をとる。締約国は、詐取する意図その他これに類する不誠実な意図を刑事責任が生ずる要件とすることができる。

(2) 逐条解説

本条は、電磁的記録の無権限作成および無権限改変を含むコンピュータ関連偽造が、証拠としての価値を侵害する行為であることにかんがみて、データ中に含まれる情報の真正性に信頼を置く法律行為の過程でなされる場合、これを偽造行為として処罰することを目的としている（EM81）。また、偽造対象であるコンピュータ・データは、私文書および公文書の別を問わない（EM83）。

国内法（電磁的記録不正作出罪・刑法第 161 条の 2）では、偽造の対象は「人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」及び「公務所又は公務員により作られるべき電磁的記録」であり、本条では、偽造の対象は「computer data」であり、何の限定も付されていない。

しかしながら、本条では「法律上の目的において真正であるとみなされ又は扱われる意図をもって」という要件があり、EM83 でも法的効果を持つものをカバーする条項であるとされ、EM84 では「法律上の目的において」とは、法律上の関係がある法的取引及び文書を指すとされている。したがって「法律上の目的において真正であるとみなされ又は扱われる意図をもって」いる場合には、概ね「人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」または「公務所又は公務員により作られるべき電磁的記録」が偽造されると思われる。したがって、本条で処罰の対象となる「computer data」は「人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」または「公務所又は公務員により作られるべき電磁的記録」と実質的に同義であると解釈することは可能であり、本条は国内法により担保可能と考えられる。

(3) 研究会における意見

本条では、有形の文書の偽造と電磁的記録の偽造を同等の犯罪行為として扱うことを可能にすることを目的としている。ネット型の電子マネーについては、有価証券に相当する電磁的記録と解釈できる限度において本条により刑法的保護がおよぶが、通貨に相当する電磁的記録というものは存在しないので、通貨偽造に対応する電磁的記録の偽造については、本条によるカバーがおよばないのではないか。

## 1.8.第 8 条　コンピュータに関連する詐欺（Computer-related fraud）

(1) 逐条

【原文】

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

(a) any input, alteration, deletion or suppression of computer data;

(b) any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

【和訳】

締約国は、自国の国内法により、自己又は他人のために、権限なしに経済的利益を得ることを不正に又は不誠実に意図して、権限なしに故意に次の行為を行い、他人に対し財産上の損害を加えることを犯罪とするため、必要な立法その他の措置をとる。

(a) コンピュータ・データの入力、改ざん、削除又は隠ぺい

(b) コンピュータ・システムの機能に対する妨害

(2) 逐条解説

本条は、他人の財産について、直接的に経済的損失またはその占有喪失を発生させ、かつ、行為者が自己または他人のために違法な経済的利益を得ることを意図してなされる不正操作行為を、犯罪として処罰することを目的としている（EM88）。

本条については、通常の詐欺について定めた刑法第 246 条、電子計算機使用詐欺罪（第 246 条の 2）およびその他の財産罪の適用により担保可能である。いわゆる内部犯行については、「他人のためにその事務を処理する者」が、図利加害目的で任務違背行為を行い、財産上の損害を与えた場合には、背任罪の適用による担保も可能である。

(3) 研究会における意見

本条における「fraud」は、日本語の「詐欺」ということばよりも意味する範囲が広く、日本においては窃盗にあたる犯罪も含むと考えられる。実際上、多くの場合は、通常の詐欺行為の手段としてコンピュータ・ネットワークを利用しているだけであり、通常の詐欺罪で十分に担保可能と考えられる。ID・パスワードの又借りについては、現行の刑法第 246 条の 2（電子計算機使用詐欺罪）で処罰の対象になるか否かについて見解が分かれるところである。たとえば、又借りした ID・パスワードで有料のサービスを利用した場合、とくにそのサービ

スにおいて人間がどのように介在するかという点がはっきりしない場合（機械が相手の場合）には、刑法第 246 条の 2 の対象となるか否かが問題となるが、「不正な指令」の解釈如何や、本条の前提の解釈如何によって、結論が分かれている。最近の学説上は、刑法第 246 条の 2 の成立を肯定する見解が有力である。この点を積極に解するときには、ブロードバンドでの有料サービスを利用した場合にも、刑法第 246 条の 2 の処罰対象となると考えられる。

## 1.9.第 9 条　児童ポルノに関連する犯罪（Offences related to child pornography）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   (a) producing child pornography for the purpose of its distribution through a computer system;
   (b) offering or making available child pornography through a computer system;
   (c) distributing or transmitting child pornography through a computer system;
   (d) procuring child pornography through a computer system for oneself or for another person;
   (e) possessing child pornography in a computer system or on a computer-data storage medium.
2. For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:
   (a) a minor engaged in sexually explicit conduct;
   (b) a person appearing to be a minor engaged in sexually explicit conduct;
   (c) realistic images representing a minor engaged in sexually explicit conduct.
3. For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

【和訳】

１．　締約国は、自国の国内法により、権限なしに故意に行われる次の行為を犯罪とするため、必要な立法その他の措置をとる。

（ａ）コンピュータ・システムを通じて配布するために児童ポルノを製造すること。

（ｂ）コンピュータ･システムを通じて児童ポルノの取得を勧誘し又はその利用を可能にすること。

（ｃ）コンピュータ･システムを通じて児童ポルノを配布し又は特定の者に送信すること。

（ｄ）自己又は他人のためにコンピュータ･システムを通じて児童ポルノを取得すること。

（ｅ）コンピュータ・システム内又はコンピュータ・データ記憶媒体内に児童ポルノを保有すること。

２．　１の規定の適用上、「児童ポルノ」とは、次のものを視覚的に描写するポルノをいう。
(ａ)　あからさまな性的なふるまいを行う未成年者
(ｂ)　あからさまな性的なふるまいを行う未成年者であるようにみえる者
(ｃ)　あからさまな性的なふるまいを行う未成年者を表現する写実的画像
３．　２の規定の適用上、「未成年者」とは、十八歳未満のすべての者をいう。ただし、締約国は、より低い年齢の者のみを未成年者とすることができるが、十六歳を下回ってはならない。
４．　締約国は、１ｄ及びｅ並びに２ｂ及びｃの規定の全部又は一部を適用しない権利を留保することができる。

(2) 逐条解説

本条は、児童ポルノグラフィの電子的な製造、所持および頒布に関連する様々な行為を、犯罪として処罰することを目的としている（EM93）。

本条は、第 2 条ないし第 8 条と同様に、故意に（intentionally）行われた場合にしか処罰されない。したがって、児童ポルノグラフィの提供、利用可能化、頒布、伝送、製造又は保有をする意図を有しない者は責任を負うことはない。例えば、ISP は刑事責任を免れるために、Web サイトや newsroom を監視する義務は負わない（EM105）。

わが国における児童ポルノグラフィに関連する様々な犯罪行為の処罰については、「児童買春・児童ポルノ禁止法（児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律）」で規定されているが、第 1 項ｃについては、児童ポルノ画像データ自体をインターネットを通じて送信する行為、および「不特定又は多数」の者に対して行う意図を有しない「特定」の者に頒布する行為が、同法で規制されておらず、担保できない。

児童買春・児童ポルノ禁止法第 2 条第 3 項にいう「児童ポルノ」は、従来より一般に有体物と解されているところ、横浜地裁川崎支判平成 12・7・6（電子メールシステム上の画像データを有体物に化体されたのと同視して「図画」に該当するとして、「猥褻物」概念を拡張解釈）の考え方に立てば、児童ポルノをデータとして送信することも現行法で処罰の対象となると解する余地はある。尤も、最決平成 13・7・16 は、「わいせつな画像データを記憶、蔵置させたホストコンピュータのハードディスクは、刑法第 175 条が定めるわいせつ物に当たるというべきである」としており、これに従えば児童ポルノデータ自体を児童ポルノと解することには困難が生じることになろう。いずれにせよ、児童ポルノデータを「物」と解すること自体は解釈として疑問が残る以上，同項の「児童ポルノ」の定義規定を改正し、児童ポルノ画像データが含まれることを明文で追加するか、又は児童ポルノデータをコンピュータ・システムを通じて送信することを処罰する規定を創設する等、新たな刑事立法を行うことが本来望ましいものと解される。

第 1 項ｄおよび e、ならびに第 2 項 b および c については、わが国の国内法が規制の対象としていない類型であるから、第 4 項の規定に基づいて、それらを適用しない権利を留保しなければならない。

(3) 研究会における意見

児童ポルノに情報を含むか否かという点の解釈については、川崎支部判例、最高裁判例のいずれが今後の主流となっていくかという問題もさることながら、そもそも定義規定それ自体が明確性を欠いているという問題も看過されてはならない。

米国においては、児童ポルノの配布、送信についての規制をめぐって、憲法訴訟がおきており、「表現の自由を侵害する」という違憲判決が出た場合には、本条による規制が人権保障に反するのではないかという点が、正しく問題となる。この点に関しては、たしかに「児童ポルノは特別である」旨の連邦最高裁判例が存在するが、米国も本条についてはなお留保の可能性がある。

## 1.10. 第 10 条　著作権及び関連する権利の侵害に関する犯罪
（Offences related to infringements of copyright and related rights）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

【和訳】

1. 締約国は、自国の国内法により、文学的及び美術的著作物の保護に関するベルヌ条約の千九百七十一年七月二十四日のパリ改正条約、知的所有権の貿易関連の側面に関する協定及び著作権に関する世界知的所有権機関条約に基づいて課された義務に従って自国の法令に定める著作権（これらの条約によって付与された著作人格権を除く。）の侵害が故意に、商業的規模で、かつ、コンピュータ・システムという手段によって行われることを犯罪とするため、必要な立法その他の措置をとる。
2. 締約国は、自国の国内法により、ローマで作成された実演家、レコード製作者及び放送

機関の保護に関する国際条約(ローマ条約)、知的所有権の貿易関連の側面に関する協定及び実演及びレコードに関する世界知的所有権機関条約に基づいて課され義務に従って自国の法令に定める関連する権利（これらの条約によって付与された著作人格権を除く。の侵害が故意に、商業的規模で、かつ、コンピュータ・システムという手段によって行われることを犯罪とするため、必要な立法その他の措置をとる。

３．　締約国は、他の効果的な救済手段が利用可能であり、かつ、その留保が１及び２に規定する国際文書に定める締約国の国際的義務に違反しない限り、限定された状況において、１及び２の規定に基づく刑事責任を課さない権利を留保することができる。

(2) 逐条解説

第 1 項は、著作権侵害行為について規定したものであるが、著作権侵害行為については、著作権法第 119 条で処罰の対象となっている。

第 2 項は、著作隣接権侵害行為について規定したものであるが、著作権侵害行為については、同じく著作権法第 119 条で処罰の対象となっている。

第 3 項の留保については、現行の著作権法は、ベルヌ条約その他の条約に反するものではないと理解されているうえ、著作権法第 5 条により著作権法と条約が抵触する場合には、条約が優先して適用されることが規定されており、留保の必要もないと考えられる。

(3) 研究会における意見

特に留意すべき点はない。

## 1.11.第 11 条　未遂及びほう助又は教唆（Attempt and aiding or abetting）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.
3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

【和文】

１．　締約国は、自国の国内法により、第二条から前条までの規定に従って定められる犯罪が行われることを意図して故意にこれらの行為をほう助し又は教唆することを犯罪とするため、必要な立法その他の措置をとる。

２．　締約国は、自国の国内法により、第三条から第五条まで、第七条、第八条並びに第九条１ａ及びｃの規定に従って定められる犯罪の未遂が故意に行われることを犯罪とするため、必要な立法その他の措置をとる。

３．　締約国は、２の規定の全部又は一部を適用しない権利を留保することができる。

(2) 逐条解説

本条では、第 1 項において、第 2 条ないし第 10 条にしたがって定められる各犯罪の正犯に対する幇助または教唆を犯罪化することを規定し、また、第 2 項において、第 3 条、第 4 条、第 5 条、第 7 条、第 8 条、第 9 条（1）(a) および（1）（c）にしたがって定められる各犯罪の未遂を犯罪化することを規定している。ただし、第 3 項の留保を付することにより、上記の各犯罪の全部または一部について、未遂を犯罪化しないことが認められている EM118－122)。

未遂については、国内法で犯罪化されていない部分もあるが、第 3 項の留保を付することにより、未遂を処罰対象から除くことが認められているから、担保可能である。

(3) 研究会における意見

特に留意すべき点はない。

## 1.12. 第 12 条　法人の責任（Corporate liability）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
   (a) a power of representation of the legal person;
   (b) an authority to take decisions on behalf of the legal person;
   (c) an authority to exercise control within the legal person.
2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

【和文】

１．　締約国は、個人として又は法人の機関の一部として活動する自然人であって、法人内部で指導的立場にあるものが、次のいずれかの権限に基づき、かつ、法人の利益のためにこの条約に従って定められる犯罪を行う場合に当該行為についての責任を当該法人に負わせ得ることを確保するため、必要な立法その他の措置をとる。
   (ａ)　法人の代表権
   (ｂ)　法人の代理として決定を行う権限
   (ｃ)　法人の中で管理を行う権限
２．　１に規定する場合を除くほか、締約国は、自然人が法人の権限に基づき活動する者が法人の利益のためにこの条約に従って定められる犯罪を行う場合において、当該犯罪が１に規定する自然人による監督又は管理の欠如によるものであるときは、当該法人に責任を負わせ得ることを確保するため、必要な措置をとる。
３．　締約国の法的原則に従い、法人の責任は、刑事上、民事上又は行政上のものとすること

ができる。

４．　このような責任は、当該犯罪を行った自然人の刑事責任に影響を及ぼすものではない。

(2) 逐条解説

本条は、企業の利益のために指導的立場にある者によって実行された犯罪行為について、法人に対して責任を課すことを目的としている。また、犯罪行為が法人の従業員や代理人によって実行された場合においても、当該法人に監督、管理の責任が負わされるべきことが示されている（EM123)。

本条に基づく責任は、「効果的で均衡がとれたかつ抑止力のある」制裁（sanction）という基準（第 13 条第 2 項）に適合するものであれば、刑事責任、民事責任、または行政的制裁とすることが、締約国の法原則に従い選択可能である（EM126)。また、第 4 項において、本条の定める法人の責任が、当該犯罪を行った自然人の刑事責任を排除するものでないことが明言されている（EM123－127)。

日本の民事上の損害賠償は本条第 3 項でいう民事上の責任に含まれ、かつ民法第 44 条（法人の不法行為能力）が全ての法人に適用されるとの解釈に立てば、国内法による担保は可能である。

(3) 研究会における意見

条約における民事上の責任は civil penalty のようなものを意味しており、わが国における損害賠償を第 13 条の制裁（sanction）の一種であると解釈することには疑問があるとの意見もある。刑事責任、民事責任、または行政的制裁とすることが締約国の法原則に従い選択可能となっているのは、ドイツのように法人の刑事責任を認めていない国の存在を考慮しているからであるとも考えられる。法人の刑事責任を肯定している日本においては，法人の責任は刑事責任でなければならないとすれば、大きな改正が必要となるとの指摘があった。

なお、本論点については起草過程においても議論があり、通常の民事上の損害賠償責任をもって担保することをもって十分であることが議場で確認されているとの指摘が事後的に事務局からなされた。

## 1.13. 第 13 条　制裁及び措置（Sanctions and measures）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

【和文】

1. 締約国は、第二条から第十一条までの規定に従って定められる犯罪が効果的で、均衡がとれたかつ抑止力のある制裁（自由の剥奪を含む。）によって処罰されることを確保するため、必要な立法その他の措置をとる。
2. 締約国は、前条の規定に従って責任を負う法人が、刑事上の又は刑事上以外の制裁又は措置であって、効果的で、均衡がとれたかつ抑止力のあるもの（金銭的制裁を含む。）を課されることを確保する。

(2) 逐条解説

本条では、犯罪条約の第 2 条ないし第 11 条に基づいてその処罰が定められるべき各犯罪行為について、「効果的で、均衡がとれたかつ抑止力のある制裁」が、当該犯罪行為に対する責任を負うべき自然人または法人（第 12 条）に課されるべきこと（自然人の場合は、拘束刑を含むものとされる（EM128））を求めている。

国内法における刑罰および制裁を、「効果的で、均衡がとれたかつ抑止力のある制裁」であると解釈することにより、本条は担保可能である。

(3) 研究会における意見

制裁の態様として「自由の剥奪を含む」という文言に関して、かかる制裁をいかなる場合に設けるべきかという点は、「効果的な（effective）」ないし「抑止力のある（dissuasive）」という条件が、「自由の剥奪」を常に要求するか否かという解釈の問題である。語義上は必ず含む必要があるという意味ではないと解される余地がないでもないが、本条が司法共助および犯罪人引渡しの問題を視野に入れたものであると考えるときには、一定期間以上の自由刑が必要ということになり、実際上は刑種・刑期についての制約がかかると考えられる。

## 1.14. 第 14 条　手続規定の適用範囲（Scope of procedural provisions）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
   (a) the criminal offences established in accordance with Articles 2 through 11 of this Convention;
   (b) other criminal offences committed by means of a computer system; and
   (c) the collection of evidence in electronic form of a criminal offence.
3.
   (a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
   (b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
      (i) is being operated for the benefit of a closed group of users, and
      (ii) does not employ public communications networks and is not connected with another computer system, whether public or private,

   that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

【和文】

１．　締約国は、特定の捜査又は刑事手続のためにこの章に規定する権限及び手続を設定するため、必要な立法その他の措置をとる。

２．　第二十一条に特に別段の定めがある場合を除くほか、締約国は、次の事項について１に

規定する権限及び手続を適用する。

(a) 第二条から第十一条までの規定に従って定められる犯罪

(b) コンピュータ・システムという手段によって行われる他の犯罪

(c) 犯罪の電子的形態の証拠の収集

3. (a) 犯罪又はその種類の範囲が、第二十一条に規定する措置を適用する犯罪の範囲より制限的でない場合には、締約国は、留保において特定する犯罪又は、その種類についてのみ第二十条に規定する措置を適用する権利を留保することができる。締約国は、同条に規定す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。

(b) 締約国は、この条約の採択の時に有効な法令による制限によって、第二十条及び第二十一条に規定する措置を次のシステムを有するサービス・プロバイダのコンピュータ・システム内での通信に適用することができない場合には、このような通信にこれらの措置を適用しない権利を留保することができる。

(i) 閉鎖したグループのユーザーのために稼働しているシステム

(ii) 公共通信ネットワークを利用せず、かつ、公的又は私的な他のコンピュータ・システムにつながっていないシステム

締約国は、第二十条及び第二十一条に規定す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。

(2) 逐条解説

本条は、刑事手続の法領域における諸々の権限および手続について、それらの適用範囲を規定している。この権限および手続の適用により、非電子的なデータと同様に、コンピュータ・データの入手および収集が可能となる。本条の定める適用範囲には 2 つの制限がある。第一は、条約第 21 条において通信内容の傍受権限を「自国の国内法に定める重大犯罪の範囲内」に限定している点である。第二は、その留保中で指定された犯罪または犯罪類型についてのみ通信記録（トラフィック・データ）のリアルタイム収集の手続を適用する権限を留保できる点である。ただし、その犯罪又は犯罪類型は、第 21 条が適用される犯罪行為の範囲よりも限定されたものであってはならない（EM140－143）。

(3) 研究会における意見

特に留意すべき点はない。

## 1.15. 第 15 条　条件及び保障条項（Conditions and safeguards）

(1) 逐条

【原文】

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

【和文】

1. 締約国は、自国の国内法に定める条件及び保障条項であって、人権及び自由（この章に規定する権限及び手続の設定、実施及び適用が、千九百五十年の人権及び基本的自由の保護に関する欧州評議会条約、千九百六十六年の国際連合の市民的及び政治的権利に関する国際規約その他の適用のある人権に関する国際条約に基づいて負う義務に従って生ずる権利を含む。）の適当な保護を規定しており、かつ、比例原則を含むものに従うことを確保する。
2. １に規定する条件及び保障条項には、関連する権限又は手続の性質を適切に考慮して、特に、司法上の又は他の独立した監督、適用を正当化する根拠並びにこのような権限又は手続の範囲及び期間に関する制限を含む。
3. 締約国は、公共の利益、特に司法の健全な運営と一致している限り、この章に規定する権限及び手続が第三者の権利、責任及び合法的利益に対して及ぼす影響を考慮する。

(2) 逐条解説

本条は、本章に規定する刑事手続上の権限および手続の制定、施行、適用にあたって、各締約国の国内法によって提供される「人権および基本的自由の保障」および「均衡の原則」といった、上位規範による要請に従うべきことを規定している（EM144－147）。

(3) 研究会における意見

特に留意すべき点はない。

## 1.16.第 16 条　蔵置されたコンピュータ・データの迅速な保全
（Expedited preservation of stored computer data）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

【和文】

1. 締約国は、特定のコンピュータ・データが滅失又は改ざんに対して特に弱いと信ずるに足りる理由がある場合には、自国の権限のある当局が、当該コンピュータ・データ（トラフィック・データを含む。）であってコンピュータ・システムという手段によって蔵置されたものの迅速な保全を命じ又はこれに類する方法により迅速な保全を確保することを可能にするため、必要な立法その他の措置をとる。
2. 締約国は、ある者が保有し又は管理している特定の蔵置されたコンピュータ・データを保全するよう当該者に命ずることによって１の規定を実施する場合には、自国の権限のある当局がそのコンピュータ・デ一タの開示を求めることを可能にするために必要な期間（九十日を限度とする。）、コンピュータ・データの完全性を保全し及び維持することを当該者に命ずるため、必要な立法その他の措置をとる。締約国は、このような命令を引き続き更新することができる旨定めることができる。
3. 締約国は、コンピュータ・データを保全すべき管理者その他の者に対し、１及び２に規

定する手続がとられていることについて、自国の国内法に定める期間秘密のものとして取り扱うことを義務付けるため、必要な立法その他の措置をとる。

４．　この条に規定する権限及び手続は、前二条の規定に従うものとする。

(2) 逐条解説

本条は、国内の権限ある当局に対して、特定の犯罪捜査または刑事手続において、既にサービス・プロバイダなどのデータ保有者によって収集・保持されたコンピュータ・データを対象に、捜索・差押え等を実施するまで、一定期間、迅速な保全を命令する権限を与えることを目的としている（EM149、157）。ここでいう「保全」とは、すでにコンピュータ・データとして存在しているデータが、改変、劣化および削除から保護されていることをいい（したがって、一定のデータの収集や保存を義務づけるものではない（EM152））、これを実現するための適切な保全方法の決定については、各締約国に任されている。また、保全の指示は、裁判所または行政機関（例：警察又は検察官）の命令によるだけではなく、法律で定められた他の手段によることも可能とされている（EM160）。

第 2 項においては、各締約国の国内法は、保全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、また、個別の命令は、特定された当該データが保全されるべき期間を具体的に指定しなければならないことを規定している。

第 3 項においては、データを保全すべき管理者またはデータの保全を命じられた者に対し、国内法で規定する期間、保全手続が行われていることに関して、秘密保持の義務を課している（EM157－163）。

EM155 にあるように、本手続は、ほとんどの国にとって国内法上、全く新しい法的権限又は法的手続である。現行の刑事訴訟法に基づく捜索・差押えの運用を迅速に行うことで、同一の効果を実現できるとの解釈をとることも可能ではあるが（EM160）、上記 EM にもあるとおり、本条は、捜索、差押とは異なる別個の迅速な手続が想定されているものと考えられ、国内法では直接該当する条文はない。令状発付を行う「権限ある当局」については、各締約国の権利保障制度に依存するということになっており、わが国の場合は、裁判所による令状発付制度を前提とすることとなると考えられる。また、保全手続の「迅速」性については、保全命令に応対する ISP の技術的な対応が可能な範囲内ということが前提となる。

なお、この保全命令は、特定の犯罪捜査のための処分である。通信事業者等に対して、犯罪と無関係に一般的にログの保存等を義務付ける措置とは異なる。このような措置は刑事手続法規で規律する事項ではない。

(3) 研究会における意見

日本国内の状況としては、まずは裁判所による令状発付を前提とすると思われるが、司法機関に限定せずに行政機関による命令発動を可能にする制度を持つ国（米・伊・露。なお米

国及びイタリアの制度については下記注参照。）もあり、条約制定過程においては、こういった制度についても念頭に入れて検討が行われたものと考えられる。この制度の目的が、保全を要するデータを改変、劣化および削除から保護するために、そのような行為が行われる前に当該データを保全するということであれば、日本のように令状の発付が比較的迅速に行われる場合には、捜索・差押え・検証を迅速に行うことにより、条約上の義務（「これに類する方法による迅速な保全」）を果たすことはできると考えられる（EM160）。他方、条約の本来の趣旨は、捜索・差押えの要件よりも軽い要件で、とりあえずの保全を可能とすることにあると考えられ、立法論として、捜索・差押えよりも簡易なコンピュータ・データの緊急保全制度の創設も検討に値する（EM160 でも、各国において保全命令を発する権限及び刑事手続の創設を検討することが推奨されている）。

しかし、捜索・差押えの迅速な実行では足りないという実情があるのか、裁判所の命令では現行の差押えと大差ないとして、仮に捜査機関の命令による保全制度を考案するとすればどのような法的問題（特に憲法上の令状主義との抵触）、事実上の問題が生じるのか等、つめるべき事項は少なくない。他方、令状発付を前提とした場合、法律によって発付要件を捜索・差押えの場合より緩めることができるかという論点がある。この場合、捜査機関はデータそのものを取得するわけではないし、また、その内容を認識するわけでもないから、データないしその化体された媒体に対する捜索、差押えの場合よりも緩和された要件の制度を創設することも論理的には可能とも考えられるが、実際の制度については、我が国の現行制度の運用、比較法的検討も踏まえた更なる検討が必要である。

条約の担保として、立法は不可欠ではないと思われるが、条約の条文を素直に読めば、コンテンツ・データとトラフィック・データの取扱いは截然と区別され、コンテンツ・データについてはともかく、トラフィック・データについては、簡易な保全（第 16 条）と犯人の迅速な追跡に資するための開示（第 17 条）を認めておくことが、国際司法共助が絡む場面で要請される可能性があり、各国の対応によっては、日本のみ迅速な捜索・差押えで対処すれば足りるとは限らないとも考えられる。

保全手続の運用上の問題としては、犯罪条約で要求する迅速性がどの程度のレベルかという点がある。ISP の立場としては時間的、技術的に対応できない要求に対して罰則規定が設けられた場合には問題であり、法が不可能を強いるような事態に陥らないよう、命令の要求内容について慎重な考慮が必要である。

＊米国における保全命令制度の概要：
合衆国法典第 18 編第 2703 条 (f) により、プロバイダ等は、政府機関の要請を受けたときは、裁判所の命令その他の令状が発布されるまで、記録その他の証拠を保全する義務が課される。保全すべき期間は、90 日間であるが、政府機関の再度の要請があれば、更に 90 日間保全しなければならないものとされている。米政府の説明によると、政府機関の要請は書面または口頭で行うことが可能であり、いかなる政府機関も要請が行える。

＊イタリアにおける保全命令制度の概要（イタリア政府の説明によるもの）：
イタリアにおいては、刑事訴訟法第 252 条によって本制度が定められている。記録その他の証拠が保全対象であり、裁判官または検察官の発する書面のみにより保全命令が可能である。

## 1.17.第 17 条　通信記録の迅速な保全及び部分開示
（Expedited preservation and partial disclosure of traffic data）

(1) 逐条

【原文】

1　Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

(a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

(b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2.　The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

【和文】

１.　締約国は、前条の規定に基づいて保全される通信記録について、次のことを行うために、必要な立法その他の措置をとる。

(a) 当該通信の送信に関与したサービス･プロバイダが一であるか二以上であるかにかかわらず、通信記録のこのような迅速な保全が利用可能となることを確保すること。

(b) 当該通信が送信されたサービス･プロバイダ及び経路を自国が特定することができるようにするため、自国の権限のある当局又はその当局によって指名された者に対して十分な量の通信記録の迅速な開示を確保すること。

２.　この条に規定する権限及び手続は、第十四条及び第十五条の規定に従うものとする。

(2) 逐条解説

本条は、第 16 条の規定を前提とした、通信記録（トラフィック・データ）についての応急保全または部分開示に関する規定であり、複数のサービス・プロバイダが通信の伝送に関与した場合において、トラフィック・データの応急保全が、これら全てのサービス・プロバイダに対して有効なものとなり得ることを確保しようとするものである。また、当該通信が送信されたサービス・プロバイダ及び経路を特定するために、権限のある当局又はその当局によって指名された者に対し、保全命令またはこれに準ずる措置を受けたサービス・プロバイダが、十分な量の通信記録（トラフィック・データ）を応急的に開示することを確保すべき旨を定めている。本条においては、実現されるべき具体的な措置については特定されておら

ず、自国の法システムおよび経済システムに適合した措置の決定が、各締約国にゆだねられている（EM168）。説明用覚書で例として挙げられているのは、それぞれのサービス・プロバイダに対する応急保全の個別執行、単一命令(a single order)による関係サービス・プロバイダに対する包括的な命令、保全を命じられたサービス・プロバイダに対し、保全命令の期間内、存在するチェーンの中にある次のサービス・プロバイダへの通知の義務づけなどである（EM168）。また、サービス・プロバイダに対する保全命令によるのでは、法執行当局に通信記録（トラフィック・データ）の開示はなされないので、法執行当局は、当該保全命令の相手方となったサービス・プロバイダが決定的な通信記録の全てを保有しているのか、あるいは通信の伝送チェーンに関わる他のサービス・プロバイダが存在するのかどうかを知ることができない。そこで、本条は、当該通信が伝送された他のサービス・プロバイダ及び経路を権限ある当局が特定できるようにするため、当局又は指定された者に対し、保全命令又はこれに類する措置を受けたサービス・プロバイダが十分な量の通信記録（トラフィック・データ）を応急的に開示することを求めている（EM169）。

第 16 条と同様、現行の刑事訴訟法に基づく捜索・差押えの運用を迅速に行うことで、「応急的な開示」に相当する効果が得られるとの解釈をとることは可能であるが、同条と同様、本条の趣旨としては、捜索、差押とは異なる別個の迅速な手続が想定されているものと考えられ、国内法では直接該当する条文はない。いずれにしても、保全手続の迅速性については、保全命令に応対する ISP が技術的に可能な範囲内ということが前提となる。令状発付を行う「権限のある当局」については、各締約国の権利保障制度に依存するということになっており、わが国の法律状況にかんがみれば、裁判所による令状発付制度を前提とすることが予想される。

(3) 研究会における意見

基本的に第 16 条と同様であり、現行法での担保も可能ではあるが、本条の趣旨としては別個の制度を想定していると考えるのが自然ではある。新たな制度を創設する場合には、ISP に対し新たな情報の生成が依頼される可能性があり、民間側の負担も考慮した上での慎重な制度整備が必要である。また、本条は通信記録（トラフィック・データ）を対象とした規定となっているが、実際のコンピュータ・データについて、通信記録（トラフィック・データ）とそれ以外の部分に区分することは困難であり、定義どおりにコンピュータ・データと通信記録（トラフィック・データ）の間で異なった取扱いができるかどうかは不明である。その他の議論については、第 16 条の記述参照。

## 1.18.第 18 条　提出命令（Production order）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
   (a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
   (b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
   (a) the type of communication service used, the technical provisions taken thereto and the period of service;
   (b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
   (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

【和文】

1. 締約国は、自国の権限のある当局に対し次のことを行う権限を与えるため、必要な立法その他の措置をとる。
   (a) 自国の領域内に所在する者に対し、当該者が保有し又は管理する特定のコンピュータ・データであって、コンピュータ・システム又はコンピュータ・データ記憶媒体に蔵置されているものを提出させること。
   (b) 自国の領域内でサービスを提供するサービス・プロバイダに対し、当該サービス・プロバイダが保有し又は管理するサービスに関連する加入者情報を提出させること。
2. この条に規定する権限及び手続は、第十四条及び第十五条の規定に従うものとする。
3. この条の規定の適用上、「加入者情報」とは、サービス・プロバイダによって保有されるサービス加入者に関連する情報のうち、トラフィック・データ及びコンテント・データ

以外のコンピュータ・データその他の情報であって、それにより次のことが立証されるものをいう。

(a) 使用された通信サービスの種類、そのために使用された技術的設備及びサービスの期間

(b) サービス契約又は取極に基づいて利用可能な加入者の特定、郵便上の又は地理的な住所、電話番号その他アクセスのための番号並びに請求及び支払に関する情報

(c) サービス契約又は取極に基づいて利用可能な通信機器の設置場所に関するその他の情報

(2) 逐条解説

本条は、自国の権限ある当局に対し、領域内に所在する者から特定の記録されたコンピュータ・データを提供させる権限、および、領域内でサービスを提供しているサービス・プロバイダから加入者情報を提出させる権限を与えることを求めている。問題となるデータは、記憶され又は現存するデータであって、将来の通信に関する通信記録（トラフィック・データ）やコンテンツ・データのようにまだ存在していないデータは含まない。本条による「提出命令」は、国が犯罪捜査に関係する情報を入手する上で、データの捜索及び差押のようなシステマティックな強制措置に代えて、柔軟かつより侵害的でない措置を用意するものと位置づけられる（EM170, 171）。かかる手続メカニズムは、ISP のような第３者的なデータ管理者にとって有用となると考えられている。彼らは、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、法執行当局を自主的に支援する準備をしているが、こうした者は、そのような支援を行うに際しての適正な法的根拠を求め、そのことから生じるあらゆる契約上のあるいは非契約上の責任から逃れることを望んでいるからである（EM171）。本条に基づく提出命令は、個人又はサービス・プロバイダが当該データ又は情報を保持している限りで適用可能であるが、本条はサービス・プロバイダの中には、そのサービスの利用者に関する記録を保存していない者があることも前提としている（EM172）。第１項にいう「保有し又は管理する」とは、命令を発した締約国の領土内に関連データが物理的に保有されていること、及び提出されるべきデータが当該者の物理的な保有の外にあったとしても、その者が、命令を発した締約国の領土内から自由に当該データの提出を管理できる状況を指している（EM173）。提出の様式については、締約国は、命令中に特定された方法で、特定されたコンピュータ・データ又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、あるいはデータ又は情報が、「プレーン・テキスト」、オンライン、紙のプリントアウト若しくは磁気ディスクで提供されるものとするように、といった方式についての指示を含むことができる（EM176）。

本条でいう「加入者情報」については第 3 項で定義されており、原則として、サービス・プロバイダのサービスの利用者に関して、サービス・プロバイダの運営者が保持するあらゆる情報のことを指しているが、通信記録及び通信内容は含まない（EM177, 180）。本条は、

サービス・プロバイダに対し、その加入者の記録を保存するように義務づけるものと理解されてはならないし、サービス・プロバイダにそのような情報の正確さを要求しようとするものでもない（EM181）。本節の権限と手続は特定の刑事捜査又は刑事手続のためのものであるので（条約第 14 条）、提出命令は、個別のケースにおいて、通常は特定の加入者に関するケースにおいて用いられる。本条項は、締約国に対し、例えばデータ・マイニングの目的で、見境のない分量の、加入者グループに関するサービス・プロバイダの加入者情報の開示を命ずる法律上の命令を発する権限を付与するものではない（EM182）。また、条文においては、秘密保持についての特段の指示は含まれていないが、捜査手続の実効性を担保するためには、秘密保持に関する措置を可能な限り採ることが求められる（EM175）。

現行法では、対象者に一定の作為を法的に義務づける性格の捜査処分は想定されていないが、情報の提供を義務づける処分として公務所等に対する照会の規定（刑事訴訟法第 197 条第 2 項）で一応の担保は可能と考えられる。ただし、同項の照会に対して通信の秘密に該当する事項を回答することは不可能なこと、同項の照会は個人に対しては行えないこと等に鑑みると、捜査機関による提出命令制度の創設を検討することが必要である。

(3) 研究会における意見

国内法における捜査手続における強制処分としては、捜索・差押え・検証がありうるが、いずれについても、収集される相手に受忍を義務付けることは可能であっても、作為を強制することはできない。刑訴法第 197 条第 2 項の捜査関係事項照会により、照会の相手方を法的に義務付けることにより担保するという考え方もあり得るが、通信の秘密保護との関係で実効性に疑問がある。

実際に収集可能な情報および技術的に対応可能な範囲は、ISP によって異なっているのが現状であり、強制的に差し押えられた場合の破損の危険を避けるため、事前に紙または媒体に出力したものを任意に提出することが多い。このように、現行法における ISP 等に対する捜索・差押え（ハードディスク等の差押え）も、実態的には提出命令制度に限りなく近い運用が行われているが、対象者・関係者の権利・利益保護や、捜索・差押え処分に伴う加重な侵害を回避するという観点からも、対象者に作為を間接強制する強制処分としての提出命令制度の法制化の必要性は高いと思われる。

立法化するとすれば、より簡略な制度（捜査機関による命令＋違反に対する罰則）として設計することも検討すべきであるが、捜索・差押えに準ずる制度（関連性、特定性等の要件）として、裁判所の令状に基づく制度を設計することになるのではないかと思われる。

この場合、拒絶要件（証言拒絶との関係、なお、相手方に被疑者が含まれると「黙秘権」との関係）、違反に対する制裁のあり方など、詰めるべき点が少なくない。

提出命令については、現行刑訴法第 99 条第 2 項、第 100 条（郵便物押収）との関係の整理も必要であろう。

## 1.19.第 19 条　蔵置されたコンピュータ・データの捜索及び押収
（Search and seizure of stored computer data）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
   (a) a computer system or part of it and computer data stored therein; and
   (b) a computer-data storage medium in which computer data may be stored in its territory.
2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
   (a) seize or similarly secure a computer system or part of it or a computer-data storage medium;
   (b) make and retain a copy of those computer data;
   (c) maintain the integrity of the relevant stored computer data;
   (d) render inaccessible or remove those computer data in the accessed computer system.
4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

【和文】

１．　締約国は、自国の領域内において、自国の権限のある当局に対し次のものを捜索し又は

これに類するアクセスを行う権限を与えるため、必要な立法その他の措置をとる。

(a) コンピュータ・システムの全部又は一部及びその中に蔵置されたコンピュータ・データ

(b) コンピュータ・データを蔵置することができるコンピュータ・データ記憶媒体

2. 締約国は、自国の権限のある当局が１ａの規定に従って特定のコンピュータ・システムの全部又は一部を捜索し又はこれに類するアクセスを行う場合において、捜索するデータが自国の領域内にある他のコンピュ一夕・システムの全部又は一部の中に蔵置されていると信ずるに足りる理由があり、かつ、当該データに対して当初のシステムから合法的にアクセスが可能であるか又は当初のシステムで利用可能であるときは、当該当局が当該他のコンピュータ・システムに対して捜索又はこれに類するアクセスを速やかに行うことができることを確保するため、必要な立法その他の措置をとる。

3. 締約国は、１又は２の規定に従ってアクセスしたコンピュータ・データを押収し又はこれに類する方法で確保する権限を与えるため、必要な立法その他の措置をとる。これらの措置には、次のことを行う権限を含む。

(a) コンピュータ・システムの全部若しくは一部又はコンピュータ・データ記憶媒体を押収し又はこれに類する方法で確保すること。

(b) コンピュータ・データの複製を作成し及び保持すること。

(c) 蔵置された関連するコンピュータ・データの完全性を維持すること。

(d) アクセスしたコンピュータ・システム中の当該コンピュータ・データに対してアクセスすることができなくすること又は当該データを消去すること。

4. 締約国は、自国の権限ある当局に対し、１及び２に規定する措置をとることを可能にするために必要な情報を合理的な範囲で提供するようコンピュータ・システムの機能又はコンピュータ・システム内のコンピュ一夕・データを保護するために適用される措置に関する知識を有する者に命ずる権限を与えるため、必要な立法その他の措置をとる。

5. この条に規定する権限及び手続は、第十四条及び第十五条の規定に従うものとする。

(2) 逐条解説

本条は、自国の権限ある当局に対し、記憶されたコンピュータ・データに関して、有体物と同様の捜索および押収の権限を付与することを求めている（EM184)。有形物の捜索・差押えと比較して、コンピュータ・データの捜索の特徴として EM が挙げているのは、①データは電磁的形式といった目に見えない形式になっている、②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押収し、取り上げることができない、③データが捜索された特定のコンピュータ内には記憶されていなくても、他のコンピュータ・システムとの接続性により、そのようなデータに容易にアクセスし得るかもしれない、という３点である（以上 EM187)。「捜索又はこれに類するアクセス」という用語において、「捜索」という伝統的な用語の使用により、国家による強制的な権限の行使という概念が持

ち込まれ、かつ、本条中の権限が伝統的な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、調査を意味する。これは、データの捜索と、（調査する）データの探索という意味を含んでいる。他方で、「アクセス」という用語は、中立的な意味を持っているが、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用語法とを結合しようとして用いられている（EM191）。

第 2 項は、捜索するデータが他のコンピュータ・システムの中に記憶されていると信ずる根拠を有する場合には、捜査機関が、（その領土内に存する）当該他のコンピュータ・システム又はその一部に対してその捜索又はこれに類するアクセスを拡張することを許している（EM193）。しかし、条約は、この捜索の拡張がどのように許容され、遂行されるべきかについては特段の規定はなく、いくつかの例示が挙げられている他は、各国の判断に委ねられている（EM194）。

本条約中、「押収」とは、データもしくは情報が記録された物理媒体を取り上げること、またはデータもしくは情報の複製を作成して保持することを指す。押収されるデータの使用又はそれにアクセスするのに必要なプログラムの押収も意味している。「押収」という伝統的な用語を用いるのと並んで、コンピュータ環境の中で、無形のデータを没収し、アクセス不能にし、その他の方法でそのコントロールを奪うような他の方法を反映するために「これに類する方法で確保する」という用語が含まれている。すなわちこの用語は、データの管理を奪うこと又はデータを取り上げることを指している（EM197）。

本条第４項において、自国の権限ある当局に、システム運営者に対し、捜索および押収の支援を、合理的な範囲で強制する権限を付与することも定められている。すなわち、コンピュータ・システムについての特別の知識を有しているシステム管理者は、捜索手続がどのように行われるのが技術的方法として一番良いかについて相談に応じる必要があるかもしれないことが認識された（EM200）。EM201 では、この権限は、捜査当局に対する利益となるだけでないとされる。すなわち、そのような協力がなければ、捜査機関は、捜索を行っている間ずっと、捜索場所に居座り、コンピュータ・システムへのアクセスを妨げるかもしれない。これにより、その間データに対するアクセスを禁止される正当な企業又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、捜索をより効果的にし、費用効率をよくする助けとなるだろう。システム運営者に対して支援を法律によって強制することは、データを開示しないことについての契約上その他の義務から、システム運営者を免れさせることにもなる（EM201）。

本条は自国の領域内における捜査手続についてのみ及ぶものであり、他国の領域内にあるデータもしくは情報についての捜索および押収は射程外である（EM192）。

我が国現行法との関係については、現行の刑事訴訟法における捜索・差押えにかかる諸規定の適用により担保されているといい得る部分もあるが、現行法の差押は有体物を前提とし

たものであること、本条第 3 項（c）（d）はデータ自体の差押えが可能であることを前提としているとも考えられ、現行法による担保で十分かどうか疑義があることから、データを対象とした捜索・差押えに関する立法措置を行うことが望ましい。

(3) 研究会における意見

データの捜索・差押えについての条約上の義務は、基本的には、記録媒体に対する捜索・差押え・検証により対処が可能であり、現行法のままでも、条約上の義務を担保していると言えなくもない。しかしながら、東京地裁平成 10 年 2 月 27 日決定に見られるように（一枚のフロッピーディスクに記録されたプロバイダの顧客データのうち、被疑者に関するデータについては関連性を肯定しつつ、それ以外の会員に対するデータについては関連性を否定し、結論としてはフロッピーディスク全体について差し押さえを取り消した）、差し押さえるべきデータの量に対して、記録媒体に記録されている無関係の情報の質と量が極めて多くなる傾向があるという問題が存在することに照らせば、端的にデータ（特定の犯罪と関連性のあるデータ）そのものの捜索・差押え・検証（これらの性質を併せ持った新たな強制処分）を認めることが、特に、第３者たる ISP が絡む場合の全体の利益に適うと考えられ、また条約の本来の趣旨にも適うと考えられることから、その制度化を図ることが望ましい。

現行法は、捜索・差押えについて、場所や対象を事前に特定することを絶対的な要件としている。しかし、コンピュータ・データ自体を対象とする場合には、これまで想定していたような物理的な場所や対象を事前に特定することは困難である。したがって、データを前提とした捜索場所の特定の仕方、ネットワークでつながっている他のコンピュータへのアクセスの可否などの論点についての検討が必要となる。

さらに、捜索・差押えへの協力の義務づけが必要となると考えられる。この中には、捜索対象のデータの捜索・これを分離・抽出して複製を作成すること、プリントアウトすること、そして元データにつき、アクセス禁止又は削除などの措置を採ることが含まれる。なお、捜索・差押えといっても、性質上、対象者のコンピュータを相当程度利用することとなり、単なる受忍を超える費用が発生する可能性が高い。作為義務を法制化するに当たっては、違反に対する制裁のあり方、被疑者の場合の取扱いなど、検討すべき多くの論点がある。

第 3 項 c 号に規定される完全性の維持、d 号に規定されるコンピュータ・データにアクセスできなくすること又はその消去については、有体物による差し押さえで本条が担保されていると考えれば、特段の対応は不要であるが、データを対象とした捜索・差押えに関する立法措置を行う場合には、どのように対応すべきかが問題となる。刑事訴訟法第 111 条 1 項の「必要な処分」として許される余地もあるが、不明確であるため、さらなる検討が必要である。

また、ネットワークで接続された他のコンピュータ・システムからデータを探索する行為については、一般探索的な強制処分は憲法上許されないとされており、そのことは憲法第 35 条 2 項が「各別の令状」を要求する点にもあらわれていると解されるところ、かかる探索行為によ

って被疑事実と関連性を有する情報を獲得した場合、その捜査手段の適法性および得られた情報の証拠能力の有無の判断基準につき検討が必要である。

なお、特に、名誉毀損的な記述内容、児童ポルノ画像等が差押えの対象となる場合、これを「廃棄」することの実体法上の根拠を与えるため、「物」の没収を定める刑法第 19 条の改正も必要となるとの意見もある。

## 1.20.第 20 条　通信記録のリアルタイム収集（Real-time collection of traffic data）

(1)　逐条解説

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
   (a) collect or record through the application of technical means on the territory of that Party, and
   (b) compel a service provider, within its existing technical capability:
      (i) to collect or record through the application of technical means on the territory of that Party; or
      (ii) to co-operate and assist the competent authorities in the collection or recording of,

      traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

【和文】

１．　締約国は、自国の権限のある当局に対し、コンピュータ・システムという手段によって伝達された自国の領域内における特定の通信に関連する通信記録についてリアルタイムで次のことを行う権限を与えるため、必要な立法その他の措置をとる。
　(ａ)　自国の領域内において、技術的手段の適用を通じて収集し又は記録すること。
　(ｂ)　サービス・プロバイダに対し、その既存の技術的能力の範囲内で、次のことを強制すること。
　　(ｉ)　自国の領域内において、技術的手段の適用を通じて収集し又は記録すること。
　　(ii)　当該当局が収集し又は記録するに当たり、これに協力し及び支援すること。
２．　締約国は、自国の国内法制の確立された原則によって、１ａに規定する措置をとること

ができない場合には、当該措置に代えて、自国の領域内において技術的手段を適用することにより、当該領域内の特定の通信に関連する通信記録をリアルタイムで収集し又は記録することを確保するため、必要な立法その他の措置をとることができる。

3．　締約国は、サービス・プロバイダに対し、この条に規定する権限の行使の事実及び権限の行使に関する情報について秘密のものとして取り扱うことを義務付けるため、必要な立法その他の措置をとる。

4．　この条に規定する権限及び手続は、第十四条及び第十五条の規定に従うものとする。

(2)逐条解説

本条は、特定の犯罪に対する捜査手続の場面における、通信記録（トラフィック・データ）のリアルタイム収集及び記録について規定している。具体的には、技術的手段によって通信記録（トラフィック・データ）の収集または記録する能力を、自国の権限ある当局に確保すること、また、サービス・プロバイダに対し、通信記録（トラフィック・データ）を収集もしくは記録させる権限、または収集もしくは記録について協力または支援させる権限を、自国の権限ある当局に付与することを義務付けている。ただし、収集もしくは記録の対象となる通信記録（トラフィック・データ）は、特定の通信に関連するものである必要があり、膨大な量の通信記録（トラフィック・データ）を一般的にまたは無限定に対象とすることは認められない（EM219)。締約国は、自国の権限ある当局が第１項(a)に基づき、技術的な手段によって、通信記録（トラフィック・データ）を収集又は記録する能力を確保することを義務付けられている。同条項は、データ収集が行われる技術的な方法を特定していないし、技術的な要件に関する義務も規定されていない（EM220)。また、本条は、サービス・プロバイダに対し、通信記録（トラフィック・データ）の収集、記録、協力又は支援を、既存の技術的能力の範囲で提供することを求めているのであり、何らかの技術的能力を確保することを義務付けるものではない。また、新たな装置を入手又は開発することを求めていないし、専門家を雇用したり費用をかけてシステムを再構築することを求めてもいない(EM221)。第 2 項に規定されている場合を除いて、締約国は第１項(a)〔権限ある当局自らによるデータの収集又は記録〕及び(b)〔権限ある当局がサービス・プロバイダに対する強制によって実現する収集又は記録〕の双方の措置を実施可能としなければならない。第１項(b)によってサービス・プロバイダが強制されるのは、「その既存の技術的能力の範囲内」なので、仮にサービス・プロバイダが通信記録（トラフィック・データ）の収集を引き受けるだけの能力を有しないようなときは、締約国は、第１項(b)により、法執行当局が当該任務を引き受けられるようにする必要があるし、通信記録（トラフィック・データ）の収集及び記録について、第１項(b)(ii)に基づいて権限ある当局に協力すべき協力し及び支援する義務は、権限ある当局が自ら通信記録（トラフィック・データ）の収集又は記録をする権限を有していない場合には、無意味である（EM223)。しかしながら、このような二層の義務は、法執行当局がサービス・プロバイダの支援を通じてのみ通信システム内のデータを傍受することができるような国や、少な

くとも、サービス・プロバイダの知識を借りなければ内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ので、第 2 項がそのような場合について対応している。この場合、締約国はサービス・プロバイダに対し必要な技術設備の提供を強制するだけにするといったような異なるアプローチを採用することによって、法執行当局による通信記録（トラフィック・データ）のリアルタイム収集を確保することができる（EM224）。また、捜査上の秘密の保護を担保するためには、サービス・プロバイダを、加入者に対する通知義務から解除する必要がある（EM225）。そこで、第 3 項において、本条に規定する措置の実施に関する事実および情報について秘密を保持すべき義務を、サービス・プロバイダに対して負わせるために必要な措置が義務付けられている。この条項は、捜査の機密性を確保するたけではなく、サービス・プロバイダが、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又はその他の法律上の義務から、サービス・プロバイダを解放することにもなる。第 3 項は、法律上の明示的な義務の創設によって有効となるかもしれないし、他方、締約国は、当該措置について話し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のような、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（EM226）。我が国では犯人蔵匿罪（刑法第 103 条）、証拠隠滅罪（刑法第 104 条）がこれに当たる。

仮に通信記録（トラフィック・データ）のリアルタイム収集は通信傍受法で認められている範囲でしか許容されないと考えたとしても、条約第 14 条第 3 項に基づき、本条に示す措置を適用する犯罪の範囲を条約第 21 条に示す措置を適用する犯罪の範囲まで限定することができるため、我が国においては、本条についても現行の通信傍受法による担保が可能といえる。第 3 項の守秘義務については、EM226 に従えば、刑法第 103 条（犯人蔵匿等）などの規定により、刑事的に担保可能と考えることができる。

(3)研究会における意見

通信記録（トラフィック・データ）のリアルタイム収集を、現行の刑事訴訟法における検証規定の適用により行う場合、特別法である通信傍受法における傍受令状が限定的に認められている趣旨にかんがみれば、通信傍受の性質を有する強制処分については同法の許容する範囲内でのみ令状を発付できると解すべきであるから、たとえば刑訴法上の検証令状の発付を受けることは不可能ではないかとの指摘がある。例えば、通信傍受法第 16 条で傍受の最中に「トラフィック・データ」である電話番号の逆探知ができることが規定されている。それまでは逆探知について法律上の明文の根拠はなかったが、通信傍受法において、初めて許容される場合が明示的に規定されたことからすれば、少なくとも現行法においては、コンテンツもトラフィックも通信傍受法で認められている範囲内でのみ収集することが許容されていると考えられる。この見解に立てば、本条は条約第 14 条第３項(a)に基づく留保を行うことによって、通信傍受法によってのみ担保されるということになる。

他方、コンテンツ・データのリアルタイム収集については通信傍受法により、通信記録（トラフィック・データ）のリアルタイム収集については検証で担保され得るとの見解もある。しかしながら、この考え方に立ったとしても、はたして現行の検証制度で問題なく担保可能かどうか、具体的には、検証と捜索の区分、収集すべきデータの特定性の確保、未だ発生していない事実についての令状発布の可否とった点が問題とされる。また、そもそも「リアルタイム収集」については、蔵置データの迅速な保全及び開示とどのように異なるのか、技術的に可能かどうかが問題となる。また、条約は、トラフィックとコンテンツは、定義上截然と区分されることとされているが（条約第１条)、現実論としての両者の区分可能性や、通信記録（トラフィック・データ）のリアルタイム収集の捜査としての有効性・不可欠性が問題となる。

例えば、リモートで不正アクセスがなされ、WEB が今現行犯で書き換えられているという場合に、犯人をトレース・バックするには、トラフィック・データのリアルタイム収集が必要な場合があるとすれば、その場合、コンテンツの通信傍受とは異なる通信状態記録傍受制度を作る必要も生じ得ると考えられる。そこで例えば、トラフィック・データについて、傍受要件を軽減し、対象犯罪を捜査技法として不可欠な特有の犯罪に限定したような、新たな通信傍受制度の構築が想定され得る。しかしながら、本分野については、国際的にも立法の前例のない分野であり、各国の法制度の整備状況も調査しつつ、慎重な検討を行う必要がある。

また、本条第 3 項の秘密保持義務については、mail, IP レベルの話では、被疑者にリアルタイム収集が行われていることがわかってしまうという設定があり得るが、これが守秘義務違反とされると、サービス・プロバイダの観点からは問題が多いとの指摘もなされた。

## 1.21. 第 21 条　通信内容の傍受（Interception of content data）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:
   (a) collect or record through the application of technical means on the territory of that Party, and
   (b) compel a service provider, within its existing technical capability:
      (i) to collect or record through the application of technical means on the territory of that Party, or
      (ii) to co-operate and assist the competent authorities in the collection or recording of,

   content data, in real-time, of specified communications in its territory transmitted by means of a computer system.
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

【和文】

１．　締約国は、自国の権限のある当局に対して、自国の国内法に定める重大犯罪に関して、コンピュータ・システムという手段によって伝達された自国の領域内における特定の通信に関連する通信内容についてリアルタイムで次のことを行う権限を与えるため、必要な立法その他の措置をとる。

(ａ)　自国の領域内において、技術的手段の適用を通じて収集し又は記録すること。

(ｂ)　サービス・プロバイダに対し、その既存の技術的能力の範囲内で、次のことを強制すること。

(ｉ)　自国の領域内において、技術的手段の適用を通じて収集し又は記録すること。

(ii) 当該当局が収集し又は記録するに当たり、これに協力し及び支援すること。

2. 締約国は、自国の国内法制の確立された原則によって、1(a)に規定する措置をとることができない場合には、当該措置に代えて、自国の領域内において技術的手段を適用することにより、当該領域内の特定の通信に関連する通信内容をリアルタイムで収集し又は記録することを確保するため、必要な立法その他の措置をとることができる。

3. 締約国は、サービス・プロバイダに対し、この条に規定する権限の行使の事実及び権限の行使に関する情報について秘密のものとして取り扱うことを義務付けるため、必要な立法その他の措置をとる。

4. この条に規定する権限及び手続は、第十四条及び第十五条の規定に従うものとする。

(2) 逐条解説

本条は、特定の犯罪に対する捜査手続の場面における、通信内容のリアルタイム収集及び記録について規定している。その規定の仕方は、第 20 条における通信記録（トラフィック・データ）の収集又は記録、協力義務、支援義務、機密保持義務の場合と同様である。ただし、本条の適用は、通信の秘密やプライバシーを過度に侵害することがないよう、「自国の国内法に定める重大犯罪」に関する場合に限定されている（EM229）。

現行の通信傍受法においては前提犯罪が限定されているが、本条の適用は「自国の国内法に定める重大犯罪」に関する場合に限定されているので、同法の適用による担保が可能である。

(3) 研究会における意見

第 20 条の場合と同じように、通信記録と通信内容を明確に区分しうる定義づけ如何という理論的な問題と、通信内容のリアルタイム収集の具体的・技術的な実現方法如何という実際的な問題について、慎重な検討が必要である。

## 1.22. 第 22 条　裁判権（Jurisdiction）

(1) 逐条

【原文】

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
   (a) in its territory; or
   (b) on board a ship flying the flag of that Party; or
   (c) on board an aircraft registered under the laws of that Party; or
   (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

【和文】

１．　締約国は、次の場合において第二条から第十一条までの規定に従って定められる犯罪について自国の裁判権を設定するため、必要な立法その他の措置をとる。
   (ａ)　犯罪が自国の領域内で行われる場合
   (ｂ)　犯罪が自国を旗国とする船舶内で行われる場合
   (ｃ)　犯罪が自国の法令に基づいて登録された航空機内で行われる場合
   (ｄ)　犯罪が行われる場所の刑事法に基づいて処罰することが可能な場合又は犯罪がすべての国の領域の外で行われる場合において、当該犯罪が自国の国民によって行われるとき。

２．　締約国は、１ｂからｄまでの規定の全部又は一部の規定に基づいて設定された裁判権を適用しない権利又は特別な場合若しくは状況においてのみ適用する権利を留保することができる。

３．　締約国は、容疑者が自国の領域内に所在し、かつ、自国が引渡しの請求を受けたにもかかわらず容疑者の国籍のみを理由として他の締約国に当該容疑者の引渡しを行わない場合において第二十四条１に定める犯罪についての裁判権を設定するため、必要な措置をとる。

４．　この条約は、国内法に従って行使される刑事裁判権を排除するものではない。

５．　この条約に従って定められる犯罪が行われたとされる場合において、二以上の締約国が裁判権を主張するときに、関係締約国は、適当な場合には、訴追のために最も適した裁判権を有する国を決定するため協議を行う。

(2) 逐条解説

本条は、本条約第 2 条ないし第 11 条に定められた各犯罪について、自国の管轄権を設定するための基準を規定している。第 1 項(ａ)、(ｂ)、(ｃ)は属地主義に基づく基準であり、(ｄ)は属人主義に基づく基準である。属地主義は、行為者の国籍にかかわらず、当該犯罪が行われた国の法を適用しようとする立場であり、属人主義は、犯罪地の如何にかかわらず、当該行為者の母国の法を適用しようとする立場である。

第 4 項において、国内法に適合した刑事管轄権を、本条の義務以上に広い基準で設定することが承認されている。また、第 5 項において、複数の締約国が同一の犯罪についての管轄権を有する場合（ウィルス攻撃など）には、刑事訴追を効率的に行うために最適な管轄権を有する国を決定するために、それらの国々が協議することが定められている（EM232－239）。

第 1 項(ｄ)の定める積極的属人主義については、現行法における国外犯処罰規定の存否と関係して、その国内法における担保状況に問題が生じる。

この点、通信の秘密に対する罪については、日本の電気通信事業者の取扱中にかかる通信および有線電気通信が客体となるならば、侵害行為が外国から行われた場合であっても国内犯として処罰できるから、その限りでは（国外犯処罰規定がなくとも）管轄権が担保されている。しかしながら、日本の電気通信事業法は、日本で許可を受けたあるいは届出をしている電気通信事業者を対象としており、有線電気通信法は、我が国内の電気通信設備を対象としていることから、外国で日本人が通信の秘密を侵害したという場合については、電気通信事業法等による処罰は困難である。

他方、第 2 条については、不正アクセス禁止法における国外犯処罰規定を設ける必要があるが、本罪の場合には、その目的にある「犯罪の防止」、「電気通信に関する秩序の維持」、「高度情報通信社会の健全な発展」は、日本国内におけるそれに主眼を置いているとしても、不正アクセス行為の国外犯処罰規定を置くことを禁じるものではないと考えられる。

(3) 研究会における意見

長期 1 年を超える拘禁刑が定められている犯罪については、対応する国内法に国民の国外犯処罰の規定が存在しない場合、引渡しに応じなければならないということになるので、それを避けるためには国外犯処罰規定を設ける必要があるが、どのように構成要件を規定するかが問題である。

特に問題となるのが、現在我が国では電気通信事業法等の業法で規定されている通信の秘密侵害罪である。日本の電気通信事業法は、日本で許可を受けたあるいは届出をしている電気通信事業者を対象としており、有線電気通信法は、我が国内の電気通信設備を対象としていることから、外国で日本人が通信の秘密を侵害したという場合については、場所の適用範囲以前の問題として、法律の適用範囲の問題として、電気通信事業法等による処罰は困難である。現実的な選択肢としては、刑法上の信書開封罪と同様の犯罪類型を新設する中で、通信の秘密侵害に係る犯罪類型を統合することが最も適当と考えられる。

## 1.23. 第 23 条　国際協力に関する一般原則

（General principles relating to international co-operation）

(1) 逐条

【原文】

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

【和文】

締約国は、この章の規定に従い、かつ、刑事問題に関する国際協力についての関連する国際文書、統一され又は相互的な法令に基づいて合意された取極及び国内法令の適用を通じて、コンピュータ・システム及びコンピュータ・データに関連する犯罪に関する捜査若しくは刑事手続のため又は犯罪に関する電子的形態の証拠を収集するために、できる限り相互に協力する。

(2) 逐条解説

本条では、国際協力に関して、以下の 3 つの一般原則を規定している（EM240－243）。

- 「できる限り相互に」国際協力しなければならない。
- 協力義務の範囲は、コンピュータ・システム及びコンピュータ・データに関連する全ての犯罪に係る捜査ないし刑事手続、および犯罪に関連する電子的形態の証拠の収集とする。
- 協力は「この章の規定に従い」、「刑事問題に関する国際協力についての関連する国際文書、統一され又は相互的な法令に基づいて合意された取極及び国内法令の適用を通じて」実施されなければならない。

(3) 研究会における意見

特に留意すべき点はない。

## 1.24.第 24 条　犯罪人引渡し（Extradition）

(1) 逐条

【原文】

1.

(a) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

(b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognize the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7.

(a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

(b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

【和文】

1. (a) 第二条から第十一条までの規定に従って定められる犯罪が、関係締約国の法令により長期一年以上の拘禁刑又はこれよりも重い刑に処することとされている場合には、当該犯罪についての締約国間の犯罪人引渡しについては、この条の規定を適用する。

(b) 統一され若しくは相互的な法令に基づいて合意された取極又は二以上の締約国間で適用される犯罪人引渡条約（犯罪人引渡しに関する欧州条約（ETS 第二十四号）等）を基礎として、適用される最も軽い刑罰が異なる場合には、当該取極又は条約に基づいて定める最も軽い刑罰を適用する。

2. １に規定する犯罪は、締約国間の現行の犯罪人引渡条約における引渡犯罪とみなされる。締約国は、締約国間で将来締結されるすべての犯罪人引渡条約に１に規定する犯罪を引渡犯罪として含めることを約束する。

3. 条約の存在を犯罪人引渡しの条件とする締約国は、自国との間に犯罪人引渡条約を締結していない他の締約国から犯罪人引渡しの請求を受けた場合には、この条約を１に規定する犯罪に関する犯罪人引渡しのための法的根拠とみなすことができる。

4. 条約の存在を犯罪人引渡しの条件としない締約国は、相互間で、１に規定する犯罪を引渡犯罪と認める。

5. 犯罪人引渡しは、請求を受けた締約国の法令に定める条件又は適用可能な犯罪人引渡条約に定める条件に従う。これらの条件には、請求を受けた締約国が犯罪人引渡しを拒否することができる理由を含む。

6. １に規定する犯罪に関する犯罪人引渡しが、引渡しを求められている者の国籍のみを理由として又は請求を受けた締約国が当該犯罪について管轄権を有するものとみなすという理由により拒否される場合には、当該請求を受けた締約国は、請求を行った締約国の要請に応じて訴追のため自国の権限のある当局に事件を付託するものとし、適当な期間内に確定的な結果を当該請求を行った締約国に報告する。当該当局は、自国の法令に規定するこれと同等の性質を有する他の犯罪の場合と同様の方法で、決定、捜査及び刑事手続を行う。

7．　(a) 締約国は、署名の際又は批准書、受諾書、承認書若しくは加入書の寄託の際に、犯罪人引渡しのための条約が存在しない場合には、犯罪人引渡しのための請求を行い若しくは受け又は仮拘禁を行うことについて責任を有する当局の名称及び住所を欧州評議会事務局長に通報する。

(b) 欧州評議会事務局長は、締約国によって指定された当局の名簿を作成し、これを最新のものとする。

締約国は、常に名簿に記載された事項が正確であることを確保する。

(2) 逐条解説

本条は、犯罪条約の第 2 条ないし第 11 条に従って設けられる諸犯罪のうち、長期 1 年以上の拘禁刑が定められている犯罪について、その犯罪人の引渡しに係る本条の規定を適用することを義務づけている。また、関係する 2 ヶ国以上の締約国間において、本条とは別に、拘束力のある引渡条約あるいは相互協定が存在し、それが引渡しの要件として異なる刑の最低限を定めている場合には、後者の基準が適用されることが規定されている。さらに、適用可能な引渡条約または法律において定められる要件ないし条件が満たされていない場合には、要求を受けた締約国は引渡しに応じる必要がないことが規定されている（EM245－252)。

本条は、引渡しに関して、何らかの国内法の制定を義務付けるものではないので、現行法による担保という意味では問題がない。また、第１項 b 号については、当面は現行の逃亡犯罪人引渡法のスキームを適用することになるものと考えられる。

(3) 研究会における意見

本条は、第１項 a 号において、対象犯罪を「長期一年以上の拘禁刑又はこれよりも重い刑に処することとされている」ものとする旨を定めており、したがって自由刑の存在が前提とされている。

## 1.25.第 25 条　相互援助に関する一般原則

（General principles relating to mutual assistance）

(1) 逐条

【原文】

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.
3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.
4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.
5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

【和文】

1. 締約国は、コンピュータ.システム及びコンピュータ・データに関連する犯罪に関する捜査若しくは刑事手続のため又は犯罪の電子的形態の証拠の収集のために、できる限り相互に援助を提供する。
2. 締約国は、第二十七条から第三十五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。

3． 締約国は、緊急の状況において、要請を受けた締約国から請求された場合には、その後正式な確認が行われることを条件として、ファクシミリ、電子メール等の緊急の通信手段により、当該手段が適当なレベルの安全性及び認証を提供する限り（必要な場合には、暗号の使用を含む。）、相互援助又は関連する通信についての要請を行うことができる。

4． この章に別段の定めがある場合を除くほか、相互援助は、要請を受けた締約国の法令に定める条件又は適用可能な相互援助条約に定める条件に従う。これらの条件には、当該締約国が協力を拒否することができる理由を含む。当該締約国は、要請が財政に係る犯罪とみなされる犯罪に関するものであることのみを理由として、第二条から第十一条までに定める犯罪について相互援助を拒否する権利を行使してはならない。

5． この章の規定に従い、要請を受けた締約国が双罰性を相互援助の条件とする場合において、援助が求められている犯罪の基礎となる行為が当該締約国の法令によって犯罪であるときは、当該犯罪が当該締約国の法令によって要請を行った締約国と同一の種類の犯罪とされているか当該犯罪が同一の用語で定められているかにかかわらず、この条件が満たされているものとみなす。

(2) 逐条解説

本条は、犯罪捜査の相互援助に関する一般原則について規定したものである。相互援助は、原則として、その制約を可及的に除去することによって、可能な限り広汎に実現されなければならない。協力義務は、原則として、コンピュータ・システムおよびコンピュータ・データに関連する全ての犯罪に係る捜査ないし刑事手続、および犯罪に関連する電子的形態の証拠の収集の両方について適用されなければならない。

また、第 3 項は、相互援助が正式に実現するまでの手続途上において、捜査に関連する決定的な情報または証拠が消去されることを防ぐために、応急的な通信手段を使用して緊急の協力を要請することを承認し、かつ要請に対して応答するためにもまた、応急的な通信手段を使用することを承認している。さらに、第 4 項は、各国における個人の権利保障を考慮して、関係国内法令に従うべきことを定めている（EM253－259）。

相互援助については、特段の規定がある場合を除き、締約国の法令又は適用可能な相互援助条約が定める要件に従わなければならないとされていることから、国内法に対応する法令が存在する範囲において、担保可能である。

(3) 研究会における意見

例えば、カーニボーなどコンテント・データ収集システムの設置を他締約国から要請された場合は、本条第 4 項の規定により、締約国の法令が定める要件に従う必要がある。よって、日本においては、通信傍受法の条件がクリアされていることが前提となる。

### 1.26. 第 26 条　自発的な情報提供（Spontaneous information）

(1) 逐条

【原文】

1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

【和文】

1. 締約国は、この条約に従って定められる犯罪に関する捜査若しくは刑事手続の開始若しくは実施の際に自国が行った捜査の枠組みの中で取得した情報の開示が、開示を受ける締約国に役立つ可能性があると認める場合又は開示を受ける締約国がこの章の規定に基づき協力を要請することとなる可能性があると認める場合には、自国の国内法の範囲内において当該情報を事前の要請なしに他の締約国に送付することができる。
2. １に規定する情報を提供する前に、提供を行おうとする締約国は、当該情報を秘密のものとして取り扱い又は条件を付して使用することを要請することができる。開示を受ける締約国は、このような要請に応ずることができない場合には、情報の提供を行おうとする締約国に対しその旨を通報する。この場合において、提供を行おうとする締約国は、このような状況にもかかわらず情報を提供すべき否かについて決定する。開示を受ける締約国は、条件が付された情報を受領する場合には、当該条件に拘束される。

(2) 逐条解説

本条は、情報を保有している締約国が、事前の要請がない場合に、他の締約国に対してその情報を送付することを、明文で許容することによって、要請のない援助を提供するにあたっての法的根拠を付与するものである。慎重な取り扱いを必要とする情報を送付する場合には、その使用に関し秘密保持その他の条件に従うべき義務を付することができる（EM260－261）。

(3) 研究会における意見

特に留意すべき点はない。

## 1.27. 第 27 条　適用可能な国際協定が存在しない場合の相互援助の要請に関する手続
（Procedures pertaining to mutual assistance requests in the absence of applicable international agreements）

(1) 逐条

【原文】

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2. 
   (a) Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.
   (b) The central authorities shall communicate directly with each other;
   (c) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;
   (d) The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.
3. Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
4. The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
   (a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
   (b) it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
5. The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
6. Before refusing or postponing assistance, the requested Party shall, where

appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9.

(a) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

(b) Any request or communication under this paragraph may be made through the International Criminal Police Organization (Interpol).

(c) Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

(d) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

(e) Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

【和文】

１． 要請を行った締約国と要請を受けた締約国との間で有効な統一され又は相互的な法令に基づく相互援助条約又は取極が存在しない場合には、２から９までの規定を適用する。このような条約、取極又は法令の規定が適用可能な場合には、関係する締約国がこれら

の規定に代えて２から９までの規定の一部又は全部を適用することを合意したときを除くほか、この条の規定を適用しない。

２．　(ａ)　締約国は、相互援助の要請の送付及び要請に対する応答、当該要請の実施又は当該要請を実施する権限を有する当局に対する当該要請の送付について責任を有する一又は二以上の中央当局を指定する。

(ｂ)　中央当局は、直接相互に連絡する。

(ｃ)　締約国は、署名の際又は批准書、受諾書、承認書若しくは加入書の寄託の際に、この２の規定に従って指定された中央当局の名称及び所在地を欧州評議会事務局長に通報する。

(ｄ)　欧州評議会事務局長は、締約国によって指定された中央当局の名簿を作成し、これを最新のものとする。締約国は、常に名簿に記載された事項が正確であることを確保する。

３．　この条の規定による相互援助の要請は、要請を受けた締約国の法令と両立しない場合を除くほか、要請を行った締約国が定める手続に従って実施される。

４．　要請を受けた締約国は、第二十五条４の規定に基づき相互援助を拒否する理由に加えて、次の場合に相互援助を拒否することができる。

(ａ)　当該要請が、要請を受けた締約国が政治犯罪又はこれに関連する犯罪と認める犯罪に関連する場合

(ｂ)　要請を受けた締約国が、当該要請の実施により自国の主権、安全、公の秩序その他の重要な利益を害されるおそれがあると認める場合

５．　要請を受けた締約国は、当該要請に基づく措置が自国の権限のある当局が行う捜査又は刑事手続を害することとなる場合には、当該措置をとることを延期することができる。

６．　援助を拒否し又は延期するに先立ち、要請を受けた締約国は、当該要請を行った締約国と協議した後、適当な場合には、当該要請の一部を認めるか自国が必要と認める条件に従って当該要請を認めるかについて検討する。

７．　要請を受けた締約国は、当該要請を行った締約国に対して援助の要請の実施についての結果を速やかに通報する。要請を拒否し又は延期する場合には、拒否又は延期の理由を示さなければならない。また、要請を受けた締約国は、要請を行った締約国に対して当該要請を実施することができない理由又は当該要請の実施を著しく遅延させるおそれのある理由を通報する。

８．　要請を行った締約国は、当該要請を受けた締約国が当該要請の実施に必要な範囲を除くほか、この章の規定に基づく要請の事実及び内容を秘密のものとして取り扱うことを求めることができる。当該要請を受けた締約国は、当該要請を秘密のものとして取り扱うことができない場合には、速やかにその旨を当該要請を行った締約国に通報するものとし、当該要請を行った締約国は、このような状況にもかかわらず当該要請を実施すべきか否かについて決定する。

９．　(ａ) 緊急の場合には、相互援助の要請又はこれに関連する通報は、当該要請を行った締約国の司法当局が当該要請を受けた締約国の司法当局に直接行うことができる。このような場合において、当該要請を受けた締約国の中央当局に対し、当該要請を行った締約国の中央当局を通じて当該要請の写しを送付する。

(ｂ) この９の規定に基づく要請又は通報は、国際刑事警察機構を通じて行うことができる。

(ｃ) ａの規定に基づく要請が行われたが、要請を受けた司法当局が当該要請を取り扱う権限を有していない場合には、当該司法当局は、当該要請を自国の権限のある当局に委託し、当該委託の事実を直接当該要請を行った締約国に通報する。

(ｄ) この９の規定に基づいて行われる要請又は通報（強制的な措置を除く。）は、当該要請を行った締約国の権限のある当局が当該要請を受けた締約国の権限のある当局に直接行うことができる。

(ｅ) 締約国は、署名の際又は批准書、受諾書、承認書若しくは加入書の寄託の際に、効率性のため、この９の規定に基づく要請については自国の中央当局が行うことを欧州評議会事務局長に通報することができる。

(2) 逐条解説

本条は、要請を行う締約国と要請を受ける締約国との間に、統一的または互恵的な法律に基づく相互援助に関する条約または協定が存在しない場合には、本条所定の手続ないし条件を適用することを義務づけている。具体的には、相互援助を提供するための中央当局の創設、条件の付与、延期又は拒絶の手続、要請についての機密保持および直接連絡のルール等を規定している（EM262－274）。

第 2 項 a 号で規定されている中央当局については、国際捜査共助法第 3 条により、外務大臣が中央当局として指定されているので、既存の国内法による担保が可能である。

(3) 研究会における意見

特に留意すべき点はない。

## 1.28. 第 28 条　秘密性及び使用制限（Confidentiality and limitation on use）

(1) 逐条

【原文】

1. When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
2. The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:
   (a) kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
   (b) not used for investigations or proceedings other than those stated in the request.
3. If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.
4. Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

【和文】

1. 要請を行った締約国と要請を受けた締約国との間に、有効な統一され又は相互的な法令に基づく相互援助条約又は取極が存在しない場合には、この条の規定を適用する。このような条約、取極又は法令の規定が適用可能な場合には、関係締約国がこれらの規定に代えてこの条の規定の一部又は全部を適用することを合意する場合を除くほか、この条の規定を適用しない。
2. 要請を受けた締約国は、次のいずれかの条件が満たされる場合には、当該要請に関する情報又は資料を提供することができる。
   (a) 当該要請が、秘密保持の条件なしでは法律上の相互援助の要請に応じられない場合に秘密が保持されること。
   (b) 当該要請が要請書に記載された捜査又は刑事手続以外の捜査又は刑事手続に使用されないこと。
3. 要請を行った締約国は、２に定める条件に従うことができない場合には、速やかにその旨を他の締約国に通報するものとし、当該他の締約国は、このような状況にもかかわら

ず情報を提供するか否かについて決定する。要請を行った締約国は、当該条件を受け入れた場合には、当該条件に拘束される。

４．　２に定める条件に従って情報又は資料を提供する締約国は、当該条件に関連して、提供する情報又は資料の使用についての説明を他の締約国に要求することができる。

(2) 逐条解説

本条は、要請を行う締約国と要請を受ける締約国との間に、統一的または互恵的な法律に基づく相互援助に関する条約または協定が存在しない場合における、とりわけ慎重な取り扱いを要する情報または資料の使用に関する制限を規定している。これにより、要請を受けた締約国は、秘密保持の条件なくしては要請に応えることができない場合には、提供される情報又は資料について、秘密が保持されるべきことを要求することができる。また、被要請国は、要請書中に特定された犯罪の捜査ないし刑事手続以外に、当該情報または資料が使用されないことを条件とすることもできる。この使用制限の適用が認められるためには、その旨が被要請国によって明示されることが前提となる（EM275－280）。

(3) 研究会における意見

特に留意すべき点はない。

## 1.29.第 29 条　蔵置されたコンピュータ・データの迅速な保全
（Expedited preservation of stored computer data）

(1) 逐条

【原文】

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
2. A request for preservation made under paragraph 1 shall specify:
   (a) the authority seeking the preservation;
   (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
   (c) the stored computer data to be preserved and its relationship to the offence;
   (d) any available information identifying the custodian of the stored computer data or the location of the computer system;
   (e) the necessity of the preservation; and
   (f) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.
4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.
5. In addition, a request for preservation may only be refused if:
   (a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
   (b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
6. Where the requested Party believes that preservation will not ensure the future

availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

【和文】

１．　締約国は、他の締約国に対し、コンピュータ・システムという手段によって蔵置されたデータであって、当該他の締約国の領域内に存在し、かつ、それに関連して要請を行った締約国がデータの捜索若しくはこれに類するアクセス、その押収若しくはこれに類する確保若しくはその開示を要請する意図を有しているものの迅速な保全を命じ又はその他の方法で迅速な保全を確保するよう要請することができる。

２．　１の規定に基づいて行われる保全の要請には、次の事項を明記する。

(ａ) 保全を求める当局

(ｂ) 捜査又は刑事手続の対象となっている犯罪及び関連事実の簡潔な要約

(ｃ) 蔵置されたコンピュータ・データであって保全すべきもの及び当該データと当該犯罪との関係

(ｄ) 蔵置されたコンピュータ・データの管理者又はコンピュータ・システムの所在を特定するために利用可能な情報

(ｅ) 保全の必要性

(ｆ) 締約国が、蔵置されたコンピュータ・データの捜索若しくはこれに類するアクセス、その押収若しくはこれに類する確保又はその開示のために相互援助の要請を提出しようとしていること。

３．　締約国は、他の締約国から要請を受けた場合には、特定されたデータを自国の国内法に従って迅速に保全するため、すべての適当な措置をとる。締約国は、要請に応ずるに当たり、双罰性をその保全を行うための条件として要求してはならない。

４．　蔵置されたコンピュータ・データの捜索若しくはこれに類するアクセス、その押収若しくはこれに類する確保又はその開示のための相互援助の要請に応ずる条件として双罰性を要求する締約国は、第二条から第十一条までの規定に従って定められる犯罪以外の犯罪に関して開示の時点で双罰性という条件が満たされないと信ずるに足りる理由がある場合には、この条の規定に基づき保全のための要請を拒否する権利を留保することができる。

５．　要請を受けた締約国は、４の規定に加え、次の場合にのみ当該要請を拒否することがで

きる。

(ａ) 当該要請が、要請を受けた締約国が政治犯罪又はこれに関連する犯罪と認める犯罪に関連する場合

(ｂ) 要請を受けた締約国が、当該要請の実施により自国の主権、安全、公の秩序その他の重要な利益を害されるおそれがあると認める場合

６． 要請を受けた締約国は、保全が当該要請に係るデータの将来的な利用を確保せず当該データの秘密性を脅かし又は要請を行った締約国の捜査を害するであろうと信ずる場合、要請を行った締約国に対し速やかにその旨を通報するものとし、当該要請を行った締約国はこのような状況にもかかわらず当該要請を実施すべきか否かについて決定する。

７． １に規定する要請に応ずるために実施された保全は、要請を行った締約国が蔵置されたコンピュータ・データの捜索若しくはこれに類するアクセス、その押収若しくはこれに類する確保又はその開示のための要請を提出することができるようにするため六十日以上の期間維持する。当該データは、当該要請を受けた後、これに関する決定が行われるまでの間引き続き保全される。

(2) 逐条解説

本条は、蔵置されたコンピュータ・データの迅速な保全に関して、犯罪条約第 16 条が規定するところと同様の権能を、国際的にも実現することを目指している。蔵置されたコンピュータ・データの迅速な保全を要請することを認めるとともに、その保全要請の具体的方式について規定している。保全の提供の条件として、双罰性を要求することはできないのが原則であるが、第 2 条ないし第 11 条以外の犯罪に関しては、双罰性要件に基づく留保を付することが認められる。また、要請拒否の条件、被要請国の通報義務、データの保全期間についても規定している（EM282－289）。

(3) 研究会における意見

国際捜査共助法第 2 条第 4 号の「不可欠性」の要件を満たさない要請について、相互援助を拒否できるかどうかについては検討が必要である。

その他には、第 16 条と同様の議論がある。

## 1.30. 第 30 条　保全された通信記録の迅速な開示
（Expedited disclosure of preserved traffic data）

(1) 逐条

【原文】

1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
2. Disclosure of traffic data under paragraph 1 may only be withheld if:
   (a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
   (b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

【和文】

１．　特定の通信に関する通信記録の保全のために前条の規定に基づいて行われた要請の実施の過程において、要請を受けた締約国は、他の国のサービス・プロバイダが通信の伝達に関与していたことを発見した場合には、要請を行った締約国に対し、当該通信が伝達されたサービス・プロバイダ及び経路を特定するために十分な量の通信記録を迅速に開示する。

２．　１の規定に基づく通信記録の開示は、次の場合にのみ行わないことができる。

(a) 当該要請が、要請を受けた締約国が政治犯罪又はこれに関連する犯罪と認める犯罪に関連する場合

(b) 要請を受けた締約国が、当該要請の実施により自国の主権、安全、公の秩序その他の重要な利益を害されるおそれがあると認める場合

(2) 逐条解説

本条は、保全された通信記録（トラフィック・データ）の応急開示に関して、犯罪条約第 17 条が規定するところと同様の権能を、国際的にも実現することを目指している。これにより、被要請国は、要請国に対して、他の国に所在するサービス・プロバイダおよびその通信経路を確認するために十分な量の通信記録（トラフィック・データ）を、迅速に開示する義務を負う。ただし、被要請国は、開示することによって、自国の主権、安全、公序その他の重大な利益が害されるおそれがあると認める場合には、通信記録（トラフィック・データ）の開示を拒絶することができる（EM290－291）。

刑事訴訟法（捜索・差押え）および国際捜査共助法における関係諸規定の運用を迅速に行うことにより、国内法による担保が可能である。

(3) 研究会における意見

担保の可否とは別の問題であるが、迅速な令状発付を実現するための制度整備として、裁判官の 24 時間対応を可能にするなどの裁判所法の改正についても検討が必要であるという意見もある。また、将来的には、保全命令の規定を立法的に整備することが望ましい。

その他には、第 17 条と同様の議論がある。

## 1.31.第 31 条　蔵置されたコンピュータ・データへのアクセスに関する相互援助
（Mutual assistance regarding accessing of stored computer data）

(1) 逐条

【原文】

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.
2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.
3. The request shall be responded to on an expedited basis where:
   (a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
   (b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

【和文】

1. 締約国は、他の締約国に対し、当該他の締約国の領域内にあるコンピュータ・システムという手段によって蔵置されたデータ（第二十九条の規定に従って保全されたデータを含む。）の捜索若しくはこれに類するアクセス、その押収若しくはこれに類する確保又はその開示を要請することができる。
2. 要請を受けた締約国は、第二十三条に規定する国際文書、取極及び法令の適用を通じ、かつ、この章の他の関連規定に従って、当該要請に応じなければならない。
3. 要請を受けた締約国は、次の場合には、緊急に当該要請に応じなければならない。
   (a) 関連するデータが滅失又は改ざんに対して特に弱いと信ずるに足りる理由がある場合
   (b) 2 に規定する文書、取極及び法令に緊急の協力についての別段の定めがある場合

(2) 逐条解説

本条は、犯罪条約第 19 条を前提として、相手国の領域内に所在するコンピュータ・システムを手段として記憶されたデータについて、その捜索もしくは捜索と類似するアクセス、その押収もしくは押収と類似する確保、又はその開示を行うよう、当該相手国に相互援助を要請することを認めている。また、被要請国は、相互援助を緊急に提供する能力を確保することが求められる（EM292）。

第 1 項、第 2 項については、国際捜査共助法第 8 条が定める捜索・差押え・検証を適用することにより、国内法による担保が不可能ではない。

(3) 研究会における意見

第 19 条と同様の議論がある。

## 1.32. 第 32 条　同意に基づく又は公的に利用可能な蔵置されたコンピュータ・データへの国境を越えるアクセス

（Trans-border access to stored computer data with consent or where publicly available）

(1) 逐条

【原文】

A Party may, without the authorization of another Party:

(a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

(b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

【和文】

締約国は、他の締約国の許可を得ることなく、次のことを行うことができる。

(ａ) 公に利用可能な蔵置されたコンピュータ・データが地理的に所在する場所にかかわらず、当該データにアクセスすること。

(ｂ) 他の締約国に所在する蔵置されたコンピュータ・データをコンピュータ・システムを通じて開示する法的権限を有する者の合法的かつ任意の同意が得られる場合には、自国の領域内におけるコンピュータ・システムを通じて、当該データにアクセスし又はこれを受領すること。

(2) 逐条解説

本条は、同意に基づく場合、又は公然と入手可能な場合における、コンピュータ・データに対する国境を越えたアクセスについて規定したものである。当該コンピュータ・データがその領域内に存在する国（アクセスを受ける国）は、アクセスを行う国によって採られる一方的な措置について、拒否・処罰・苦情等によって対抗することは認められない（EM293－294）。

国内法で、本条の規定するアクセス行為を禁止する法令は存在せず、担保可能である。

(3) 研究会における意見

本条ｂ項は、法的権限の所在についての確認を要することを前提としており、ある国の捜査機関が他国で捜査活動を行うことが、それが任意処分であるというだけで当然に可能になるわけではない。

## 1.33.第 33 条　通信記録のリアルタイム収集に関する相互援助
（Mutual assistance in the real-time collection of traffic data）

(1) 逐条

【原文】

1. The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.
2. Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

【和文】

1. 締約国は、コンピュータ・システムという手段によって伝達された自国の領域内における特定の通信に関連する通信記録をリアルタイムで収集することについて、相互に援助を提供する。２の規定に従うことを条件として、援助は、国内法に定める条件及び手続によって行う。
2. 締約国は、国内の類似の事件において利用可能な通信記録のリアルタイム収集が利用可能な場合には、少なくともこのような援助を提供する。

(2) 逐条解説

本条は、自国の領域内におけるリアルタイムの通信記録（トラフィック・データ）の収集について、国際的な相互援助の提供を義務付けている。ただし、援助を提供する場合の要件ないし条件については、自国の刑事法領域における、司法共助を規定する適用可能な条約、協定、または法令に従うこととされている（EM295－296）。

刑事訴訟法（検証）および国際捜査共助法における関係諸規定の運用を迅速に行うことにより、国内法による担保が可能である。

(3) 研究会における意見

第 20 条と同様の議論がある。

## 1.34. 第 34 条　通信内容の傍受に関する相互援助

（Mutual assistance regarding the interception of content data）

(1) 逐条

【原文】

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

【和文】

締約国は、適用される条約及び自国の法令によって認められている限度において、コンピュータ・システムという手段によって伝達された特定の通信の通信内容をリアルタイム収集し又は記録することについて、相互に援助を提供する。

(2) 逐条解説

本条は、各締約国の適用可能な条約および国内法の許容する範囲内で、通信内容の傍受のための相互援助を義務付けている。相互援助義務の範囲および限界については、既存の相互援助の枠組みおよび国内法に委ねられている（EM297）。

「国内法によって認められている範囲内で」という制限があり、立法が義務付けられているわけではないので、国内法による担保について問題は生じえない。

(3) 研究会における意見

現行法上、捜査共助として通信傍受を行うことは認められていないので、通信傍受に関連する相互援助は行わない。

## 1.35.第 35 条　二十四/七ネットワーク（24/7 Network）

(1) 逐条

【原文】

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
   (a) the provision of technical advice;
   (b) the preservation of data pursuant to Articles 29 and 30;
   (c) the collection of evidence, the provision of legal information, and locating of suspects.
2.
   (a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
   (b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.
3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

【和文】

1. 締約国は、コンピュータ・システム及びコンピュータ・データに関連する犯罪に関する捜査若しくは刑事手続のため又は犯罪の電子的形態の証拠の収集のために速やかに援助することを確保するため、週七日、一日二十四時間の体制で利用可能な連絡部局を指定する。その援助には、次のことを促進することを含み又は、国内法及び慣行によって認められている場合には、次のことを直接行うことを含む。
   (a) 技術上の助言を提供すること。
   (b) 第二十九条及び第三十条の規定に従いデータを保全すること。
   (c) 証拠を収集し、法的情報を提供し、及び被疑者の所在を探すこと。
2. (a) 締約国の連絡部局は、他の締約国の連絡部局と迅速に通信する能力を有するものとする。
   (b) 締約国が指定する連絡部局は、国際的な相互援助又は犯罪人引渡しについて責任を有する当該締約国の当局でない場合には、当該責任を有する当局と迅速に調整を行

うことができることを確保する。

３．　締約国は、ネットワークの運用を促進するため、訓練され、かつ、装備を備えた要員が利用可能となることを確保する。

(2) 逐条解説

本条は、第 1 項の規定する技術的な助言の提供、データの保全、証拠の収集、法的情報の提供および被疑者の所在特定といった事項に関連して、捜査ないし刑事手続における迅速な援助を実現することを目的に、週 7 日、24 時間ベースで利用可能なネットワークを設立することを、締約国に対して義務付けている。本条で設けられるチャネルは、Ｇ８諸国において設置された既に機能しているネットワークで得られた経験に基づいている。このネットワークの設立は、本条約によって提供される捜査手段の中で、最も重要なものの一つであると考えられている（EM298）。各加盟国は、この 24/7 コンタクトポイントを法執行構造内のどこに設置するかの自由を有する（EM300）。

第 2 項においては、24/7 コンタクトポイントそれ自体が有するわけではない権能を実現するために、当該権能を有する関連当局と迅速に協働する能力を確保することが求められている（EM301）。さらに、第 3 項においては、その運営を円滑に行うための適切な装置の設置、および構成要員の十分な訓練が求められている（EM302）。

週 7 日、24 時間ベースで利用可能なネットワークは、現在すでに警察に存在しており、国内における担保は可能である。

(3) 研究会における意見

特に留意すべき点はない。

## 2.現行法で担保されていない条項の担保の方法についての試案

サイバー犯罪条約中、現行の国内法では条約上の義務を担保できていない又は担保されていない可能性が高いと考えられる条項について、これを担保するために必要な立法措置について研究会で検討を行ったところ、実体法については以下の試案が、手続法については検討の方向性、検討すべき論点の整理が得られた。

### 2.1. 実体法

#### 2.1.1. 条約第 6 条関係

【担保されていない行為】

スタンドアロン・コンピュータを対象とするシステム妨害（第 4 条）・データ妨害（第 5 条）を行うために使用する意図をもって、コンピュータ・システムへのアクセスを可能とするコンピュータ・パスワード、アクセス・コードまたはこれらに類するデータについて、それらを製造、販売、使用のための調達、輸入、配布またはその他の方法によって利用可能とする行為及び保有する行為　［第 6 条第１項(a)(ii)(b)］。

【試　案】

電磁的記録毀棄罪、電子計算機等使用業務妨害罪について準備罪を新設する。

すなわち、電磁的記録毀棄罪、電子計算機等使用業務妨害罪を実行する目的で、コンピュータ・システムへのアクセスを可能とするコンピュータ・パスワード等のデータを製造、提供、販売、譲渡、貸し渡し、輸入する行為を処罰する規定の新設を検討する。

この場合、条約上必ず担保法制の整備を行うことが必要な、システム妨害・データ妨害目的の単なるパスワード等の製造、配布行為等のみならず、近年の「不正プログラム」に起因するコンピュータ・ウィルス、不正アクセス事例の増加に鑑みれば、条約上は留保も可能であるが、電磁的記録毀棄罪、電子計算機等使用業務妨害罪を実行する目的で、同罪の結果を発生されるコンピュータ・ウィルス等の「不正プログラム」の製造、提供、販売、譲渡、貸し渡し、輸入する行為の処罰化［第 6 条第１項(a)(i)(b)］も検討する必要がある。その際、「不正プログラム」は、インターネットを介して容易に国境を超えて伝播するものであることから、我が国だけが罰則を導入することは実効性が低いことに鑑み、サイバー犯罪条約加盟国を始めとする各国における取組状況を精査した上で、海外との整合性のとれた法制度の導入を検討する必要がある。平成 14 年 3 月現在に確認できた範囲では、不正プログラムの製造・譲渡等を、実際に生じた損害とは無関係に処罰する立法があるのは、フランス（ただし未施行）、スイス（以上、サイバー犯罪条約署名国）、中国、韓国など少数であるが、現在立法化を検討中の国もあると考えられ、引き続き海外動向の調査分析が必要である。

なお、「不正プログラム」自体の製造、保有、配布等に係る許可・届出制といった行政規制の導入については、①行為者の意図、実際の被害を離れては「不正プログラム」の定義を客観的に行

うことは困難であるが、意図を問題にした場合には許可制・届出制は機能せず（「不正の意図を有してプログラムを作るものは許可を受けること」という規制は無意味）、他方、客観的要件だけで「不正プログラム」を定義しようとすると、規制範囲が著しく広くなり過剰な規制となること、②「不正プログラム」は、インターネットを介して伝播し、かつインターネットには国境がないことから世界的に整合性のとれた法制度の導入でなくては意味がないが、届出制という法制は例がないこと、③国内だけに閉じた行政規制、とりわけ事前規制の導入は、国内の情報セキュリティ関係の研究機関、企業に不要・過大な負担を課し、我が国の研究開発力、産業競争力を阻害する結果をもたらすことになるので、オプションとして相当ではない。

### 2.1.2. 条約第 9 条関係

【担保されていない可能性が高い行為】

児童ポルノ画像自体をインターネットを通じて送信する行為。

［第 9 条第 1 項ｃ］

【試　案】

児童買春・児童ポルノ禁止法第 2 条第 3 項における「児童ポルノ」の定義規定（「写真、ビデオテープその他の物」）を改正し、児童ポルノ画像データが含まれることを明文で追加するか、又は児童ポルノデータをコンピュータ・システムを通じて送信することを処罰する規定を創設する等の新たな刑事立法を行う。

### 2.1.3. 条約第 22 条関係

【担保されていない行為】

①　日本人が外国で通信の秘密を侵害する行為

②　日本人が外国で不正アクセス禁止法違反の行為を行う行為

【試　案】

①　刑法上の信書開封罪（刑法第 133 条）と同様の犯罪類型を新設する中で、通信の秘密侵害に係る犯罪類型を統合し、当該犯罪について国民の国外犯処罰規定を設ける。

②　不正アクセス禁止法に国民の国外犯処罰規定を新設する。

## 2.2. 手続法

### 2.2.1. 条約第 16 条・第 17 条関係

【担保されていない可能性がある手続】

捜索・差押えを実施するまでの間、蔵置されたコンピュータ・データで、滅失又は改ざんに弱いと考えられるものの迅速な保全をサービス・プロバイダに求める手続及び関連する他のプロバイダを同定するために通信記録の応急開示を求める手続を創設するという手続が、条約上は本来想定されていると考えられる。

【検討すべき論点】

条約の担保として、現行の刑事訴訟法に基づく捜索・差押えの運用を迅速に行うことによって、本条が達成しようとした効果を事実上達成できるとの解釈をとれば、立法化は不可欠ではないと考えられるが、条約の本来の趣旨に適った制度を構築しようとする場合であっても、以下の論点の検討が必要となる。

① 我が国の実務においては、諸外国に比べても令状発付が迅速に行われているとの指摘がある中で、本条の担保として捜索・差押えの迅速な実行では足りないという実情があるのか。仮に、簡易・迅速な特別な手続を設けるとしても、裁判所の命令を要するとすれば、結果的に差押えと大差ないことにならないか。

② 他方、国際司法共助を前提とした場合には、トラフィック・データの簡易な保全・開示を求められる可能性があり、その場合、捜索・差押え手続だけで対応可能か。

③ 「迅速」な保全という場合、どこまで「迅速」な対応ができるかは、事業者の技術に依存する部分が大きい。しかしながら、これを根拠として、事業者に一定の技術の保持が義務付けられるべきではないし、不可能な対応を強いることのないよう、制度設計には慎重な考慮が必要である。

### 2.2.2. 条約第 18 条関係

【担保されていない可能性が高い手続】

コンピュータ・データの提出命令手続

【検討の方向性】

対象者・関係者の権利・利益保護や、捜索・差押え処分に伴う加重な侵害を回避するという観点からは、対象者に作為を間接強制する強制処分としてのコンピュータ・データの提出命令の制度の法制化の必要性は高いと考えられる。その際、当該命令に基づく場合には、電気通信事業法等に基づく通信の秘密侵害罪等に係る事業者の法的責任が阻却されることが明確化される必要がある。

### 2.2.3.条約第 19 条関係

【担保されていない可能性が高い手続】

コンピュータ・データの捜索・押収手続き

【検討の方向性】

コンピュータ・データの記録媒体に対する捜索・差押え・検証により、条約上の義務を担保することも可能とは考えられる。

しかしながら、東京地裁平成 10 年 2 月 27 日決定に見られるように（一枚のフロッピーディスクに記録されたプロバイダーの顧客データのうち、被疑者に関するデータについては関連性を肯定しつつ、それ以外の会員に対するデータについては関連性を否定し、結論としてはフロッピーディスク全体について差し押さえを取り消した)、差し押さえるべきデータの量に対し、記録媒体に記録されている無関係の情報の質と量が極めて多くなる傾向があるという問題が存在することに照らせば、端的に、特定の犯罪と関連性のあるデータそのものの、捜索・差押え・検証（これらの性質を併せ持った新たな強制処分）を創設することが、不必要な権利侵害を避ける上で必要であり、特に第三者たる ISP が関係する場合に全体の利益に適うと考えられる。

その際には、捜索・差押えへの協力の義務づけの検討が必要となる。この中には、捜索対象のデータの捜索、これを分離・抽出して複製を作成すること、プリントアウトすること、そして元データにつき、アクセスの禁止又は削除などの措置を採ることが含まれる。

### 2.2.4.条約第 20 条・第 21 条関係

【担保されていない可能性が高い手続】

通信記録（トラフィック・データ）のリアルタイム収集

【検討すべき論点】

(1) 通信傍受法との関係

通信記録（トラフィック・データ）のリアルタイム収集を、通信傍受の性質を有する強制処分と解した場合、通信傍受法において傍受令状が限定的に認められている範囲内でのみ許容可能との考え方が導かれるのではないか。そうであれば、リアルタイム収集については、我が国においては、コンテンツ・データ、トラフィック・データともに、通信傍受法の枠組みにしたがった傍受のみが認められるという結論となる。

(2) 仮に、通信記録（トラフィック・データ）のリアルタイム収集については、通信傍受法で認められている場合以外にも実施し得ると考えた場合、現行の検証制度での対応と、新たな法制度の整備という二つの方向が考えられる。

① 検証で対応する場合

・ 未だ発生していない事実について、将来犯罪が発生する蓋然性に基づいて令状を発付し、検証を行うことは、少なくとも現行法を前提とする限り難しいのではないか。

・ 仮にそれが可能だとしても、検証の対象となる通信記録（トラフィック・データ）をどのように特定するのか。例えば、犯罪が行われている蓋然性が存在すれば、特定人あてのメールのトラフィックの記録を全て記録することが可能となるのか。

② 新たな制度を創設する場合

・ そもそも、条約が前提としているコンテンツ・データとトラフィック・データの区分が技術的に容易に可能なのか。容易に可能でない場合、そのような区分を行っていないビジネスモデルに対して、当該区分を前提とした手続を適用しようとすると、事業者側に実質的に新たな技術上の義務を課すことにならないか。

・ 仮に、メールサーバに記録されるのを待ち受けてデータを取得するとすると、それは、傍受ではなく、捜索・差押えの対象となるのではないか。

## 3. 各国法制度の現状

本章においては、欧州サイバー犯罪条約に係わる各国法制度の現状について概観する。
欧州サイバー犯罪条約は、刑事実体法と刑事手続法から構成されるため、本章においてもそれに準ずる。

### 3.1. 刑事実体法に係わる各国法制度の現状

本節では、G8 各国を中心に、刑事実体法に係わる法制度の現状について述べる。特に、わが国における立法を検討する際重要と考えられる第 2 条の不正アクセスに関する記述、第 6 条の不正プログラムの製造・頒布等に関する記述を中心に述べる。
全体の動向に関しては、以下の通りである。

(1)不正アクセス行為について
コンピュータへの不正アクセス行為については、いずれの国においても、犯罪として規定されている。

(2)不正プログラムの製造・頒布について
不正プログラムの製造･頒布を明確に禁止している国は、フランス（ただし未施行）、イタリア、ロシア等である。必ずしも明確な規定が存在しない国も多い。

#### 3.1.1. アメリカ合衆国
(1)不正アクセス行為について
連邦政府法では、刑法に関連規定が存在し、第 1030 条および第 2701 条に記述されている。第 1030 条には、何らかのセキュリティ措置がなされているコンピュータに意図的に無権限でアクセスし、何らかの被害を発生させた場合に関する罰則規定が存在する。
さらに、第 2701 条に、意図的にかつ無権限で、電子的な通信サービスを提供する設備にアクセスすることに関する罰則規定が存在する。
具体的には、以下の通りである。
第 1030 条においては、それぞれ不正アクセス行為の定義とそれに対する行為に関して、以下のように記述されている。

（行為の定義）
無権限で，または，授与されたアクセス権限を超過して，コンピュータにアクセスしていることの認識を持ちながら，合衆国によって保護されている情報等を保持するための手段として，意欲して，通信等をした者
意図して，かつ，無権限で，または，授与されたアクセス権限を超過して，コンピュータにアクセスし，そして，それによって，金融機関の情報等を入手した者

意図して，合衆国の省庁もしくは政府機関の非公開コンピュータにアクセスする権限なしに，合衆国政府の利用のため省庁もしくは政府機関が専用で利用するコンピュータにアクセスした者
（処罰）
罰金刑もしくは 10 年以下の拘禁刑，または，併科
再犯の場合には，罰金刑もしくは 20 年以下の拘禁刑，または，併科

また、第 2701 条においては、以下の記述がある。

（行為の定義）
意図して，かつ，無権限で，電子的な通信サービスを提供する設備にアクセスした者，または，意図して，上記設備にアクセスする権限を超過して，かつ，その権限超過によって，当該システム内の電子的な記憶の中にある間，有線通信もしくは電子通信に対する権限に基づくアクセスを入手した者，改変した者，または，妨害した者
（処罰）
罰金もしくは 1 年以下の拘禁刑，または，併科
再犯の場合，罰金もしくは 2 年以下の拘禁刑，または，併科

さらには、州毎に各種の法律が決められており、多くの州で不正アクセス行為を犯罪とする規定が存在する。

(2)不正プログラムの製造・頒布について

連邦法においては、刑法に関連規定が存在し、第 1030 条に記述がある。
第 1030 条には、悪意を持って、不正プログラムを稼動させ、コンピュータに損害を与える行為を処罰する規定が存在する。

具体的には以下のように、第 1030 条において、行為の定義と処罰を規定している。

（行為）
認識して，プログラム，情報，コード若しくは命令の伝送を惹起させ，その行為の結果として，意図して，無権限で，保護されるコンピュータに対し損害を発生させた者
（処罰）
初犯の場合，罰金刑もしくは 5 年以下の拘禁刑またはその併科
再犯の場合，罰金刑もしくは 10 年以下の拘禁刑またはその併科

また、アリゾナ州、アーカンソー州、カリフォルニア州、フロリダ州、テネシー州、ネブラスカ州、ミネソタ州、ノースカロライナ州、ウエスト・バージニア州において、不正プログラムの製造・頒布等に係わる行為が犯罪とされている。

### 3.1.2. カナダ

(1)不正アクセス行為について

カナダにおいては、刑法第 9 部「財産権を侵害する犯罪行為」第 342 条 1 に「コンピュータの無権限使用」に関する規定が存在する。

条文は以下の通りである。

(1) 違法に，かつ，権利なく，
(a) 直接・間接に，コンピュータ・サービスを入手した者，
(b) 電磁装置，音響装置，機械装置その他の装置を手段として，直接・間接に，コンピュータ・システムの機能を傍受し，または，傍受されるようにした者，または，
(c) データもしくはコンピュータ・システムに関連して，(a)号もしくは(b)号の犯罪または第 430 条の犯罪を実行する目的で，直接・間接に，コンピュータ・システムを使用した者，もしくは，使用されるようにした者は，

陪審裁判により得る犯罪として有罪であり，10 年以下の拘禁刑によって処罰され，または，略式裁判により得る犯罪として有罪である。

（明治大学夏井教授訳）

上記条文のうち、(b)項および(c)項の、「傍受されるようにした者」、「使用されるようにした者」は、不正アクセスの幇助に関する規定であるが、具体的な行為に関しては記述が無い。

(2)不正プログラムの製造・頒布について

上記(1)で触れた刑法第 342 条に、幇助に関しても罰則規定が存在しており、不正プログラムの製造・頒布等が、不正アクセス行為の幇助に該当するという解釈は可能であるが、判例は不明である。

### 3.1.3. イギリス

(1)不正アクセス行為について

イギリスにおいては、「1990 年コンピュータの不正使用に関する法律」に関連条文が存在する。この条文においては、別の犯罪を行う目的を持って無権限で、コンピュータに何らかの機能を実行させた者に対し、略式裁判が行われた場合に処罰する規定が存在する。

具体的には、第 1 条「コンピュータ・マテリアルに対する無権限アクセス」において、以下のように述べられている。

第 1 条　コンピュータ・マテリアルに対する無権限アクセス
(1) 以下の者は，有罪とする。
(a) コンピュータ内に存するプログラムまたはデータにアクセスする意図で，コンピュータに何らかの機能を実行させた場合であって，
(b) その者が得ようとしたアクセスが無権原のものであり，かつ，
(c) その者がコンピュータに当該機能を実行させた時点において，それがコンピュータに当該機能を実行させるものであること

を知っていた場合
(2) 本条の罪を実行する行為者が有していなければならない意図は，以下のいずれかに向けられたものであることを要しない。
(a) 特定のプログラムもしくはデータ
(b) 特定の種類のプログラムもしくはデータ，または
(c) 特定のコンピュータ内に保持されているプログラムもしくはデータ。
(3) 本条の罪により有罪である者は，略式裁判により，6 月以下の拘禁刑もしくは標準量刑基準におけるレベル 5 以下の金額の罰金刑に処し，または，これらを併科する。
（明治大学　夏井高人教授訳）

上記の具体例としては、不正な配布を目的としたパスワードファイルへのアクセスを挙げることができる。

(2)不正プログラムの製造・頒布について

上記「1990年コンピュータの不正使用に関する法律」の第2条において、幇助が禁止されており、不正プログラムの製造・頒布が幇助に該当すると解釈することも可能である。ただし、この件に関する判例は不明である。

具体的には、以下の通りとなっている。

第 2 条　別の罪を実行する意図または別の罪の実行を幇助する意図でなされる無権限アクセス
(1)
(a) 本条を適用すべき犯罪行為罪を実行する意図で，または，
(b) 本条を適用すべき犯罪行為を実行すること（自身が実行する場合とそれ以外の者が実行する場合とを問わない）を幇助する意図で，
上記第 1 条の罪（無権限アクセス罪）を実行した者は，有罪である。また，本条の以下の条項においては，当該の者が実行もしくは幇助しようと意図した犯罪行為を「別の罪」として指示する。
(2) 本条は，以下のいずれかに該当する罪につき適用される。
(a) その行為についての刑罰が，法律によって定められている場合，または，
(b) その行為について，（従前，前科を有しない）21 歳以上の者に対し，5 年の拘禁刑を宣告することができる場合（または，イングランドもしくはウェールズにおいては，1980 年治安判事裁判所法（1980 年一般法律第 43 号）第 33 条により課せられる制限がなければ，そのように宣告することができる場合）。
(3) 本条においては，「別の罪」が，無権限アクセス罪と同時に実行されたか，または，その後の機会に実行されたかは，重要ではない。
(4) 「別の罪」を実行することが事実上不可能であった場合であっても，当該の者は，本条について有罪である。
(5) 本条の犯罪行為を実行した者は，以下の責任を負う。
(a) 略式裁判が行われた場合，6 月以下の拘禁刑もしくは法定の最高額を超えない金額の罰金刑に処し，または，これらを併科す

る。または
(b)　陪審裁判が行われた場合, 5 年以内の拘禁刑もしくは罰金刑に処し, または, これらを併科する。
（明治大学　夏井高人教授訳）

### 3.1.4. フランス

(1)不正アクセス行為について

フランスにおいては、刑法第 323 条にて、不正アクセスの禁止に触れている。

具体的には、以下のように規定している。

（行為の定義）
不法に，データの自動処理システムの全体又は一部にアクセスし又は滞留する行為
（処罰）
1 年の拘禁刑及び 100,000 フランの罰金刑

(2)不正プログラムの製造・頒布について

刑法第 323 条に、犯罪を犯すものと考えられる、ソフトウェア・プログラムの販売、譲渡または使用を目的とする行為に関する禁止規定が追加された。

### 3.1.5. ドイツ

(1)不正アクセス行為について

ドイツにおいては、刑法第 22 章「詐欺及び背任」第 263 条 a「コンピュータ詐欺」において、以下の条文が存在する。

(1)　自己もしくは第三者に対して違法に財産上の利益を得させることを意図して，プログラムの不正な作成，不正もしくは不完全なデータの使用，データの無権限使用，または，プログラムの実行に対する無権限介入によって，データ処理プロセスの結果に影響を与え，その結果，他人の財産を損なった者は，5 年以下の拘禁刑または罰金刑に処す。
(2)　第 263 条第 2 項ないし第 7 項の規定を準用する。（明治大学夏井教授訳）

上記は、主としてコンピュータ詐欺罪を念頭においた条文であるが、不正アクセスを念頭においた条文としては、第 202 条 a「データの探知」において、以下の条文が存在する。

(1)　不正なアクセスに対して特別の保護がなされているデータであって，自己のためのものではないデータを，権限なく，自己または他の者のために入手した者は，3 年以下の拘禁刑または罰金刑に処す。
(2)　第 1 項の意味におけるデータとは，電子的な方式，電磁的な方式その他人間が直接に知覚できない方式で記憶装置に保存されているもの，または，そのような方式で伝達されるもののみをいう。

(2)不正プログラムの製造・頒布について

第 263 条に、不正プログラムの製造・頒布に係わる規定が存在する。この条文では、悪意を持って、プログラムを不正に作成することを禁じており、頒布等に関する記述は無い。

具体的には、以下の通りである。

| |
|---|
| 自己もしくは第三者に対して違法に財産上の利益を得させることを意図して，プログラムの不正な作成，不正もしくは不完全なデータの使用，データの無権限使用，または，プログラムの実行に対する無権限介入によって，データ処理プロセスの結果に影響を与え，その結果，他人の財産を損なった者は，5 年以下の拘禁刑または罰金刑に処す。 |

### 3.1.6. イタリア

(1)不正アクセス行為について

第 617 条（電信による通信または電話による会話の違法な認識，中断または阻止）の 4 において、コンピュータ・システムおよびデータシステム間の通信を違法な手段で傍受することに関する罰則規定が存在する。公務員の不正アクセス禁止に関しては、別途第 615 条の 3 に定められている。

(2)不正プログラムの製造・頒布について

刑法第 4 款 「住居の不可侵に対する犯罪」第 615 条の 4 「コンピュータ･システムあるいはデータ･システムへのアクセス･コードの違法所持及び違法配布」に、以下の条文が存在する。

| |
|---|
| 1. 自己もしくは他人の利益を図る目的で，または，他人に損害を加える目的で，セキュリティ措置で保護されたコンピュータ･システムもしくはデータ･システムへアクセスすることのできるコードもしくはパス･ワード及びその他の手段を入手し，複製し，配布し，伝送し，譲渡した者，または，上記目的を意図した手法や手順に関する説明を提供した者は，1 年以下の拘禁刑及び 10,000,000 リラ以下の罰金刑に処す。（明治大学夏井教授訳） |

パスワードおよびそれ以外の不正アクセス手段の入手、複製、配布、伝送、譲渡、さらには、それらの説明に関しても禁じている。

### 3.1.7. ロシア

(1)不正アクセス行為について

刑法第 272 条に、コンピュータ・ネットワークへの無許可進入を取り締まる条文がある。具体的には、以下のように規定されている。

| |
|---|
| （行為の定義）<br>コンピュータ，コンピュータ・システムもしくはネットワークに適法にアクセスした者が，当該コンピュータ，コンピュータ・システムもしくはネットワークの操作方法についての利用規則に違反した結果，法によって保護されているコンピュータ情報を破壊した場合，妨害 |

| |
|---|
| した場合，改変した場合，もしくは，複製した場合<br>（処罰）<br>2 年以下の拘禁刑，180 時間以上 240 時間以下の強制労働，または，5 年以下の職業制限，現実に損害を発生させた場合には，拘禁刑を 4 年以下まで加重 |

(2)不正プログラムの製造・頒布について

刑法第 273 条に、不正プログラムの製造・頒布に係わる記述が存在する。

ソフトウェア・プログラムの作成ないしは存在するプログラムの改変が、故意に(意図的に)情報の刑罰のない(unsanctioned)破壊、妨害、改変、複写を導く、ないしは、コンピュータ、コンピュータ・システムないしはネットワークの働きを破壊する場合に刑事罰を定めている。同様の刑罰が、そのようなプログラムないしはその可読メディアの使用および拡散に対して適用される。これらの行為は、同じ条項によって3 年以下の懲役および200 以上500 以下の最低制定法月給-“MSMS”(現在では、だいたい580 から1450 アメリカドルの範囲)か有罪の人間の2 乃至5 ケ月の収入の罰金を課される。実際の損害を与えた場合には、懲役は、7 年までに増える。

### 3.1.8. 刑事実体法に係わる各国法制度の現状の総括

表 3－1 に、刑事実体法に係わる各国法制度の現状を総括する。

特に現状において、国内法との整合性を検討するうえで、非常に重要な条項である欧州サイバー犯罪条約第 2 条および第 6 条に関する法制度を中心にまとめた。

表３－１　欧州サイバー犯罪条約の刑事実体法（特に第 2 条および第 6 条）に係わる各国の法制度の現状

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造･販売･配布等） | その他特徴等 |
|---|---|---|---|---|
| 北米 | | | | |
| 米国 連邦 | 刑法 | 第 1030 条に、何らかのセキュリティ措置がなされているコンピュータに意図的に無権限でアクセスし、何らかの被害を発生させた場合に関する罰則規定が存在する。<br>第 2701 条に、意図的にかつ無権限で、電子的な通信サービスを提供する設備にアクセスすることに関する罰則規定が存在する。 | 第 1030 条に、悪意を持って、不正プログラムを稼動させ、コンピュータに損害を与える行為を処罰する規定が存在する。 | 刑法の一部が、コンピュータ犯罪法に相当する。 |
| カナダ | 刑法 | 第 342 条に、直接・間接に、コンピュータ本体および周辺機器に対するアクセス権限を取得することに関する罰則規定が存在する。 | 第 342 条に、幇助に関しても罰則規定が存在している。 | 刑法の一部で、コンピュータ犯罪に関する記載がある。 |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造･販売･配布等） | その他特徴等 |
|---|---|---|---|---|
| 中南米 | | | | |
| アルゼンチン | 刑法 | 第 157 条の 2 に、システムまたはデータのセキュリティを侵害して、個人情報にアクセスまたは漏洩することに関する罰則規定が存在する。 | 記載無し。 | サイバー犯罪法の関連条文は、個人情報保護に係わる部分のみである。 |
| チリ | 法律 19.223 | 第 2 条において、情報処理システム内のデータに対して、探索, 使用もしくは違法に探知する意図で、アクセスすることに関する罰則規定が存在する。 | 記載無し。 | 法律 19.223 は、以下の 4 条から成る。<br>1 条： システムの破壊の禁止<br>2 条：システム内の情報に対する不正アクセスの禁止<br>3 条：システムに記録されているデータの改ざんの禁止<br>4 条：システム内のデータの漏洩または流布の禁止 |
| ブラジル | 刑法 | 記載無し。 | 記載無し。 | 第 313 条に、公務員によるデータ-の挿入、プログラムの改変に関する罰則規定が存在する。 |
| ベネズエラ | 刑法 | 記載無し。 | 記載無し。 | 安全保障上および法執行上との関連で一部に記載がある。 |
| メキシコ | メキシコ連邦区(D.F.)の一般法に関連する刑法及びメキシコ合衆国の連邦法に関連する刑法 | 記載無し。（ただし、第 211 条の 2 に､無権限のものがコンピュータ・システムにアクセスし、かつデータを複製することに関する罰則規定は存在する） | 記載無し。 | 第 5 編　通信手段・郵便物に関連する犯罪、第 9 編　秘密の漏洩, 情報システム・情報機器への違法アクセス、に関連条文が存在する。 |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造･販売･配布等） | その他特徴等 |
|---|---|---|---|---|
| ヨーロッパ | | | | |
| アイスランド | 刑法 | 第 228 条に、違法な手段によりデータにアクセスすることに関する罰則規定が存在する。 | （違法な手段により、データにアクセスすることを可能とする装置を入手することに対する罰則規定が存在する） | 第 228 条が該当する。 |
| イギリス | 1990 年コンピュータの不正使用に関する法律 | 第 1 条に、コンピュータに対して、無権限で、データやプログラムに対してアクセスしようとする行為に関する罰則規定が存在する。 | 第 2 条において、第 1 条を幇助することに関する罰則規定が存在する。 | 当該法律は、9 条から成る法律である。 |
| イタリア | 刑法 | 第 617 条（電信による通信または電話による会話の違法な認識，中断または阻止）の 4 において、コンピュータ・システムおよびデータシステム間の通信を違法な手段で傍受することに関する罰則規定が存在する。<br>公務員の不正アクセス禁止に関しては、別途第 615 条の 3 に定められている。 | 第 615 条に、コンピュータ・システムまたは通信システムに損害を与える目的で、コンピュータ・プログラムを配布し、転送した者に対する罰則規定が存在する。 | 刑法第 614 条～第 617 条、第 622 条、第 623 条、第 635 条、第 640 条に関連条文が存在する。 |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造･販売･配布等） | その他特徴等 |
|---|---|---|---|---|
| エストニア | 刑法 | 第 271 条に、コンピュータ，コンピュータ・システム及びネットワークの無権限使用に関する罰則規定が存在する。 | 第 273 条に、故意によるコンピュータ・ウィルスの散布に関する罰則規定が存在する。<br>第 274 条に、コンピュータ、コンピュータ・システムまたはコンピュータ・ネットワークのパスワードを配布する行為に関する罰則規定が存在する。 | 刑法の第 14 章が「コンピュータ及び就労場所に関連する犯罪」であり、ここに総括されている。 |
| オーストリア | | | | |
| スウェーデン | | | | |
| スペイン | 刑法 | 第 197 条に、ファイル、情報、電子もしくは通信その他様々なタイプの記録中の、個人もしくはその家族に関する保存データを、無権限で、損害を発生させる目的にて、保持・使用・アクセス・改変に関して、罰則規定が存在する。 | 第 400 条に、犯罪行為の遂行を目的とする工具、機材、道具、素材、機械、コンピュータ・プログラムまたは器機を製造または保有する者に関する罰則規定が存在する。 | 刑法典のうち関連部分は、以下の通りである。<br>第 10 編　プライバシー、画像に関する権利及びアドレスの不可侵に対する犯罪<br>第 11 編　知的所有権・産業的所有権、市場及び消費者に関連する犯罪<br>第 18 編 偽造 |
| デンマーク | 刑法 | 第 263 条に、他人の秘密事項にアクセスすることに関する罰則規定が存在する。さらに、同条には、電子データ処理設備において使用するために記憶されている他人の情報もしくはプログラムに不正にアクセスすることに関する罰則規定が存在する。 | 記載無し。 | 第 21 章　公共に有害な種々の行為、<br>第 27 章　自由の侵害および名誉毀損に関連条文が存在する。 |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造･販売･配布等） | その他特徴等 |
|---|---|---|---|---|
| ドイツ連邦法 | 刑法 | 第 202 条 a に、コンピュータに蓄積されているデータを、自分または第三者のために、権限無く入手した者に関する罰則規定が存在する。アクセス自体に関する記載は無い。 | 第 263 条に「自己もしくは第三者に対して違法に財産上の利益を得させることを意図して、プログラムの不正な作成、不正もしくは不完全なデータの使用、データの無権限使用、または、プログラムの実行に対する無権限介入によって、データ処理プロセスの結果に影響を与え、その結果、他人の財産を損なった者は、5 年以下の拘禁刑または罰金刑に処す。」とある。 | 刑法第 15 章　私生活及び秘密領域に対する侵害、第 22 章　詐欺及び背任、第 23 章　文書偽造、第 27 章　器物損壊、の条文が該当する。 |
| ノルウェー | 一般市民刑法 | 第 145 条に、手紙もしくはその他の非公開の書状に違法にアクセスした者、または、他人の非公開の秘密事項にアクセスした者に関する罰則規定が存在する。さらに、保護措置もしくはこれに類するものを破壊することによって、非公開の、電子的手段その他の技術的な手段により伝送されるデータもしくはプログラムの処理装置に違法にアクセスする者に関する罰則規定も存在する。 | 記載無し。 | 第 13 章　公共の秩序および自由に対する犯罪、第 14 章　公共に危険を生じさせる犯罪、第 24 章　横領，窃盗及び不正使用、に関連条文が存在する。 |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造･販売･配布等） | その他特徴等 |
|---|---|---|---|---|
| ハンガリー | 刑法 | 記載無し。 | 記載無し。 | 第 300 条 C がコンピュータ詐欺に関する条文となっており、情報処理の結果に不当に干渉することを禁じている。 |
| フィンランド | 刑法 | 第 8 条に、他人のパスワードを用いるか、またはセキュリティシステムを不正に破って、コンピュータ・システムに進入することに関する罰則規定が存在する。 | 第 8 条では、実際に不正アクセス行為がなされなくても、コンピュータ内の情報を不正に入手するための特別な装置を用いる者に対する罰則規定が存在する。 | 刑法第 38 条が、該当する。 |
| フランス | 刑法 | データの自動処理システムに対して、詐欺的に（無権限で）アクセスし、またはそこに留まる行為に関する罰則規定が存在する。 | 第 323 条に、犯罪を犯すものと考えられるソフトウェア・プログラムの販売、譲渡または使用を目的とする行為を罰する条文が、追加された。 | |
| ベルギー | 刑法 | 第 550 条の 2 で、許可されていないことを知りながら、コンピュータ･システムにアクセスし、その状態に留まることに関する罰則規定が存在する。さらに、不正な意図をもっている場合は、罰則が重くなる。 | 記載無し。 | 第 9 編　財産に対する重罪，軽罪、第 9 編の 2 コンピュータ･システムやこうしたシステムにより記憶され，処理されまたは伝送されたデータの機密性、完全性及び可用性に対する犯罪、に関連条文がまとめられている。 |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造･販売･配布等） | その他特徴等 |
|---|---|---|---|---|
| ポーランド | 刑法 | 無権限で、書簡の開披、情報を伝送する電線への接続、または、電子的、電磁的その他の特別の情報の保護に対する侵害によって、自己に帰属しない情報を取得した者に対する罰則規定が存在する。 | 第 267 条に、アクセス権限を有しない情報を取得するために、特殊な機器を導入もしくは使用した者に関する罰則規定が存在する。 | |
| ポルトガル | 情報処理に関連する犯罪行為（1991 年 8 月 17 日法律第 109 号） | 第 7 条が不正アクセスに関する規定であり、不正な利益を得る目的で、情報処理システムもしくは情報処理ネットにアクセスする者に関する罰則規定が存在する。さらに、セキュリティ規則に違反してこうした行為を行った場合は、罰則が重くなる。 | 記載無し。 | 情報処理に関連する犯罪行為（1991 年 8 月 17 日法律第 109 号）は、全 19 条から成る関連法律である。 |
| マルタ | 刑法 | | | 第 298 条 A が通信システムの保護に関する条文である。 |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造･販売･配布等） | その他特徴等 |
|---|---|---|---|---|
| ロシア | 刑法 | 第 272 条に、コンピュータ・ネットワークへの無許可進入を取り締まる条文がある。 | 第 273 条に、不正プログラムの製造・頒布に係わる記述が存在する。ソフトウェア・プログラムの作成ないしは存在するプログラムの改変が、故意に(意図的に)情報の刑罰のない(unsanctioned)破壊、妨害、改変、複写を導く、ないしは、コンピュータ、コンピュータ・システムないしはネットワークの働きを破壊する場合に刑事罰を定めている。 | |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造･販売･配布等） | その他特徴等 |
|---|---|---|---|---|
| アフリカ | | | | |
| モーリシャス | 情報技術発展のための条項を制定するために様々な法律を改正するための法律 | この法律で、刑法の改正を定めており、刑法第 369 条に、不正アクセスに係わる行為を禁じる条文の追加を定めている。 | | |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造・販売・配布等） | その他特徴等 |
|---|---|---|---|---|
| アジア | | | | |
| インド | 2000 年情報技術法 | 第 66 条で、悪意を持った不正アクセス行為を禁止している。 | | |
| シンガポール | コンピュータ不正利用禁止法 | 第 4 条で、犯罪行為の実行を意図したアクセスまたは犯罪行為の実行を容易にすることを意図したアクセス、および第 6 条で、コンピュータ・サービスの無権限使用または傍受、をそれぞれ禁じている。 | 第 10 条に、不正アクセス行為の幇助行為を禁止する条文が存在する。 | |
| 中国 | 1994 年コンピュータ情報システム安全保護条例 | 第 20 条で、コンピュータ・システムの安全に危害を加えることを禁じており、これが該当すると考えられる。 | 第 15 条に、「コンピュータ・ウィルス及び社会の公共安全に対して危害を及ぼすプログラムその他の有害プログラムの防止・対策のための研究業務は，公安部が一括管理する」との規定が存在する。 | 1994 年コンピュータ情報システム安全保護条例と、そこで触れられているコンピュータ情報システム安全等級保護制度により、規定される。 |
| トルコ | 刑法 | 記載無し。 | 裁判上の証拠として使用する目的で、文書を生成もしくは偽造するために、自動データ処理システムの中にデータその他のコンポーネント（プログラム）を挿入することを禁じている。 | 第 2 部が情報技術に関する犯罪となっている。 |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造・販売・配布等） | その他特徴等 |
|---|---|---|---|---|
| フィリピン | 電子商取引法立法化の規則及び命令 | 第 48 条において、ハッキングまたはクラッキングを禁止している。ハッキングまたはクラッキングとは、コンピュータ・システム、サーバ、情報システムもしくは通信システムへの無権限アクセス行為、または、これらシステムの認識もしくは同意なく、これらを用いて、汚染、改変、窃盗もしくは破壊のためになされるアクセス行為のことである。 | 記載無し。 | 電子商取引法立法化の規則及び命令における第 48 条　ハッキングが該当する。 |
| マレーシア | コンピュータ犯罪法 | 第 3 条にて、コンピュータのデータまたはプログラムの入手を意図した、無権限アクセスを有罪としている。 | 第 5 条に、「コンピュータ・コンテントの無権限改変を発生させることになるだろうということを認識しつつ，何らかの行動をした者は, 有罪である。」とある。「何らかの行動」に不正プログラムの製造・頒布が含まれる可能性がある。<br>さらに、第 6 条には、「通信のための適法な権限を有する者以外の者に対し、番号、コード、パスワードその他コンピュータにアクセスするための手段を、直接または間接に、送信した者は、有罪である。」とある。 | コンピュータ犯罪法が該当する。 |

| 国または州名 | サイバー犯罪法に関連する法律 | サイバー犯罪条約第 2 条関連条文の解説(論点：不正アクセス) | サイバー犯罪条約第 6 条関連条文（論点：不正プログラムまたはデータの製造･販売･配布等） | その他特徴等 |
|---|---|---|---|---|
| オセアニア | | | | |
| オーストラリア | 1989 年コンピュータ犯罪法 | 第 76 条に、連邦のコンピュータまたは連邦のためのデータを持っているコンピュータ、の有しているデータに対して、故意にかつ無権限でアクセスしたものに関する罰則規定が存在する。 | 記載無し。 | 1989 年コンピュータ犯罪法が該当する。 |
| オーストラリアタスマニア州法 | 1924 年刑法 | 第 257 条 D に、コンピュータ，コンピュータ・システム，または，コンピュータ・システムの一部へのアクセスを意図して，違法に実行する者は，有罪である。 | 第 257 条 E で､コンピュータまたはコンピュータ・システム内に、プログラムを不正に導入することを禁じている。 | 第 28 章 A が、コンピュータ関連犯罪に該当する部分である。 |

## 3.2.刑事手続法に係わる各国法制度の現状

本節では、欧州犯罪条約第 16 条、第 17 条、第 18 条、第 19 条、第 20 条にて触れられている、通信記録等の保全、および通信傍受に関して、G8 各国の法制度の動向について述べる。

全体の動向は、以下のようにまとめることが可能である。

(1)通信記録等の保全に関して

- G8 各国中で、関連法規の存在は 5 ヶ国（米国、フランス、イタリア、ドイツ、イギリス）に認められる。
- 必ずしも裁判官が発布する令状が必要の無い要件構成となっている。
- 費用負担を、常に通信事業者に求めるとは限らない。

(2)通信傍受に関して

- 緊急避難の場合を除き、裁判官の令状発付が条件となっている（米国の愛国者法を除く）。
- 令状請求に対する令状発付の割合は、何れの国も非常に高い。
- 傍受期間は、数日～数ヶ月程度となっているが、延長請求は無限に可能であり、実質的に制限はない。
- 対象とする犯罪は、非常に幅広い。

表 3－2 において、G8 各国の通信記録の保全と通信傍受の動向に係わる動向を総括する。

表３－２　欧州サイバー犯罪条約第 16 条～第 21 条に係わる G8 各国の法整備の状況

| 国名 | 欧州サイバー犯罪条約データの保全（第 16 条、第 17 条）提出命令（第 18 条）捜索および押収（第 19 条）に係る各国の法律 | | リアルタイム収集（第 20 条）通信傍受（第 21 条） |
|---|---|---|---|
| | 個人 | 通信事業者 | |
| アメリカ合衆国 | （刑法）<br>合衆国法典集第 18 款犯罪及び刑事手続第 1 部犯罪第 47 章詐欺及び虚偽の文言第 1029 条アクセス装置と関係する詐欺行為及び関連行為(c)刑罰にて、「不正アクセス行為」を行った者に対する刑罰として、拘禁刑や罰金刑とともに、犯罪の実行のために使用され、または使用するつもりであった個人財産の合衆国国庫への没収が規定されている。 | （刑法）<br>合衆国法典第 18 編第 2703 条により、プロバイダ等は、政府機関の要請を受けたときは、裁判所の命令その他の令状が発付されるまで、記録その他の証拠を保存する義務が課される。保存すべき期間は、90 日間であるが、政府機関の再度の要請があれば、更に 90 日間保存しなければならないものとされている。この規定は、捜査のための通信傍受並びに蓄積された有線及び電子的通信へのアクセス等を定めた 1986 年電子通信プライバシー法によって改正された連邦刑事法典に、1995 年包括的テロ防止法によりさらに追加されたものである。<br><br>なお、合衆国法典第 47 編第 1002 条により、事業者は犯罪捜査のための通信傍受のための設備を設置する義務を負うが、1995 年通信事業者捜査支援法では、当該設備の設置に要した費用については、政府から補償を受けることができる旨が定められている。<br><br>上記以外の通信データの保全に関する要点は、以下のとおりである。<br>・ 要請を行う政府機関は、全ての政府機関である<br>・ 要請は、口頭でも文書でもよい<br>・ 通信事業者は、無線通信事業者およびプロバイダが含まれる<br>・ | （憲法）<br>合衆国憲法修正第4条において、捜査機関による捜索・押収は適正な手続きに基づかねばならないと定められている。しかし、通信傍受に関しては、20世紀初頭においては、通常の捜索のように「物理的侵入」が存在しないため、修正第4条が適用されないと解釈されていた。しかし、オルムステッド事件・オズボーン事件・バーガー事件・カッツ事件等を通して、捜査機関による通信や会話の傍受は、適正な手続きに基づいて行われることが義務付けられるという法理が確立していると認識されている。<br>（「1968年総合的犯罪防止及び街路の安全に関する法律」）<br>連邦法においては、「1968年総合的犯罪防止及び街路の安全に関する法律」により、私人による通信傍受を原則禁止とし、捜査機関による通信傍受手続きを定めている。また、各州において通信傍受に関する手続きを定めた法律が制定されている。<br>連邦法における手続きは、以下を要点としている。<br>・ プライバシーに対する合理的期待が存在する場合、憲法修正第4条に基づく裁判所が発行した令状が必要であること<br>・ 裁判所の令状発行は、「一応の証拠」による捜索・押収活動を支える「相当な理由」が存在する場合に限られる<br>・ 令状には、押収すべき場所・物が特定されていること<br>・ ただし、適法な逮捕に伴う捜査、自動車の捜索、同意の場合、緊急性を要する場合には、事前審査に基づく令状の発付に関する例外が存在する<br>・ 傍受期間は30日であり、延長の要求が回数無制限に認められる<br>・ 犯罪に関する特定の通信（逃亡犯罪人の所在に関する通信を含む）を対象とする。傍受の対象でない通信の傍受は，最小限となるような方法により執行されなければならない<br>（州法等）<br>また、連邦政府および26の州においては、傍受件数や傍受内容について、各年毎に議会への報告が義務付けられており、毎年1月に合衆国裁判所が報告書を発表している。<br>（愛国者法）<br>2001年11月に制定されたに「H.R.3162 USAパトリオット法」において、以下が記述されている。<br>・ 単一の電話だけでなく、外国人テロリスト容疑者が使うすべての電話を傍受可能にする「ロービング傍受」の裁判所命令を連邦当局の取得を認める。<br>・ テロ容疑者の電子メール通信についてインターネット・サービス・プロバイダ（ISP）から記録を求める召喚状取得を法執行機関に認める。<br>・ ほとんどの通信傍受・諜報規定を4年で無効にする。 |

| 国名 | 欧州サイバー犯罪条約データの保全（第 16 条、第 17 条）提出命令（第 18 条）捜索および押収（第 19 条）に係る各国の法律 | | リアルタイム収集（第 20 条）通信傍受（第 21 条） |
|---|---|---|---|
| | 個人 | 通信事業者 | |
| イギリス | | （電気通信法）<br>インターネットプロバイダは、電気通信法に基づき、電気通信事業者として許可を受けなければならないこととされており、裁判所の令状発付を条件として情報を提供する義務が課せられている。<br><br>（DTI の規則案）<br>また、貿易産業省（ＤＴＩ）が、ＥＵ電気通信個人データ保護指令をイギリス国内で実施するために公表した規則案において、トラフィック・データの扱いについて以下のように規定されている。<br>トラフィック・データは、原則として、当該通信の終了の時点で消去され、かつ匿名にされなければならない。また、トラフィック・データの処理は、課金、顧客からの問い合わせ、不正行為の探知、又は関連する者による電気通信サービスのマーケティングの場合に限定される。しかし、紛争処理のための権限を有する者にトラフィック・データを提供することは許される。犯罪の捜査又は防止、刑事手続、裁判所の令状への対応等では事業者に対し、義務を課すものではない。<br><br>（刑事訴訟法[警察・刑事証拠法]）<br>1984 年の刑事訴訟法では、捜査機関は、差押え権限の一内容として、コンピュータに記録された情報を閲読可能な状態で提出するよう命ずる権限を有する。 | （通信傍受法）<br>1985 年に通信傍受法が制定された。国務大臣が、国家の安全のため、もしくは重大な犯罪の防止若しくは発見のため，又連合王国の経済の安定のため令状が必要であると認める場合に、捜査機関による通信傍受が可能とされている。ただし、緊急の場合は、その省の職員にも発付許可を与えている。他の特徴は、以下の通りである。<br>・ 傍受期間は、原則として 2 ヶ月間である（ただし、省の職員発付の者は 2 日間）<br>・ 更新は、1 ヶ月、2 ヶ月、6 ヶ月の 3 種類がある<br>・ 傍受範囲は、令状において特定され若しくは記載される特定の者，又は令状において特定され若しくは記載される特定の場所への又はこれからの通信の伝送のために利用される可能性のアドレスである。<br>・ さらには、令状において特定される 1 又は複数のアドレスへ又はこれから送られる通信，及びその他の通信である<br>・ なお，裁判所又は司法的機関における手続において，令状が発せられたこと若しくは発せられること等を示唆する証拠を提出することができず，また，尋問において，これを示唆する質問をすることができない。<br><br>（2000 年捜査権限規制法）<br>2000 年に 2000 年捜査権限規制法が制定され、傍受条件の細分化が行われた。<br>この法律の対象は、公共郵便サービスまたは公共もしくは私設の電気通信システムを利用した伝送過程にある通信としている。そして、英国内のいかなる場所においても、通信を故意にかつ法的な権限なく傍受することを違法としている。通信の傍受が認められる場合は、国際協定による場合、通信の一方の当事者が同意している場合、通信事業者が運営に必要な傍受を行う場合、無線通信に関する特別の条件に当てはまる場合、傍受令状による場合となっている。<br>傍受令状の請求・発付の手続き、令状の内容・有効期間・取消・更新、執行等に関して規定されている。さらには、傍受の性能の維持、傍受費用の供与、傍受素材に関する保障措置、無権限な開示の禁止等が規定されている。<br>なお、暗号化された電子データの捜査に関する予防型の規定、通信傍受コミッショナ、情報機関コミッショナ等の制度による国民の権利保護に特徴がある。 |
| イタリア | | （刑事訴訟法）<br>刑事訴訟法第 255 条においてデータの保全に関する記述が存在する。以下に概要を示す。<br>・ 裁判官または検察官の書面による要請による<br>・ 遠隔通信サービス、プロバイダ等が要請の対象となる<br>・ 裁判権の管轄外のデータに関しては明確になっていない<br>・ 裁判権の管轄外のプロバイダに対しては要請を行う旨の記述がある<br>・ 省庁横断的な専門家委員会が保全費用に関する基準を決定する<br>・ 通信事業者は、刑事的にも民事的にも免責される<br>・ 個人情報保護法とは、コンフリクトする | （刑事訴訟法）<br>刑事訴訟法第 266 条～第 271 条に規定されており、予審判事の発する令状に基づき傍受が行われる。5 年以上の禁固刑または終身刑に相当する犯罪、麻薬・銃器・爆発物・禁輸品の取引、傷害及び脅迫、電話による迷惑行為に対する捜査に対して発付される。組織犯罪の場合は手続きが緩和される。傍受期間は 15 日以内であり更新請求が可能である。<br>なお、1996 年には、44000 件の傍受令状が発付されている。<br>上記以外の通信傍受手続きの概要は、以下のとおりである。<br>・ 電話，ファックス，コンピュータ通信等の電気通信のほか，通信機器を介しない直接の会話を傍受の対象とする<br>・ 罪の重大な兆候が認められ、かつ捜査の続行のため傍受が絶対必要である場合に認められる<br>・ 傍受期間は 15 日以内であるが、何度でも更新請求が可能である<br>・ 聖職者、弁護士、医師、またはその他の職業上の守秘義務規定に服する職務に従事する者については、傍受の対象外となっている<br>・ 令状の発付は、予備捜査担当裁判官により行われる（緊急の場合、検察官の判断により傍受は可能であるが、48 時間以内に令状の請求を行わなければならない） |

| 国名 | 欧州サイバー犯罪条約データの保全（第 16 条、第 17 条）提出命令（第 18 条）捜索および押収（第 19 条）に係る各国の法律 | | リアルタイム収集（第 20 条）通信傍受（第 21 条） |
|---|---|---|---|
| | 個人 | 通信事業者 | |
| カナダ | （刑法）<br>刑法典第 342 条 2(2)に、コンピュータの無権限使用により有罪とされた場合、当該犯罪行為の実行に関連していた道具や装置を、国が没収することを命ずることができ、その命令に基づき、国務長官は処分する、との記述がある。 | （刑法）<br>刑法同第 342 条 2(3)には、、(2)に基づく没収が命ぜられることはない、との記述がある。通信事業者自身が犯罪行為を行っていない場合、没収されることはない。 | （刑法）<br>1974 年刑法第 4 篇において、重大犯罪の捜査・予防・訴追を目的としての、捜査機関による通信傍受が認められている。通信傍受の概要は、以下のとおりである。<br>・ 電話，ファックス，コンピュータ通信等の電気通信を対象としている<br>・ 対象とする犯罪が非常に多岐に及びことに特色がある<br>・ 令状の発付は、上級裁判所の裁判官その他所定の裁判官によってなされる<br>・ 令状発付の要件は、許可することが司法の運営に最も利益になり、かつ他の捜査方法が試みられたが失敗し，他の捜査方法が成功する見込みがなく、又は緊急事態のため他の捜査方法を行うことが実際的でないことである<br><br>（安全保障のための諜報活動法）<br>「安全保障のための諜報活動法」により、国家の安全保障目的での傍受が認められている。 |
| フランス | | （電気通信法）<br>刑事訴訟法典に基づく手続によるほか、電気通信担当大臣により授権を受け、又は、政令の規定により宣誓した電気通信担当行政機関・電気通信規制機関・周波数庁は、電気通信事業者に対し、郵便電気通信法又は同法規則に基づいて、必要な情報の提供又は資料の提出を求めることができることとされている（第 32 の 3 条、第 40 条）。<br>しかし、ネットワーク事業者及びアクセス事業者には、捜査機関に提出するために通信履歴を保存しておく義務はない。<br><br>（情報処理、ファイル及び個人の諸自由に関する法律）<br>1978 年に制定された同法においては、個人情報の収集・記録・保存についての個人の権利保障、アクセス権・訂正権等の承認、コンピュータ処理のみならずマニュアル処理・機械処理についても一定の保護がなされること等が記載されている。特徴がある。同法の適用を監視するための独立行政機関として、「情報処理及び自由に関する国家委員会(CNIL)」が設置されている。ＣＮＩＬは、その任務の遂行のため、規則制定権を有するほか、立入検査、刑事告発、苦情申立ての受理等を行うことができる。 | （法律名不明）<br>1991 年に制定された法律により、捜査機関の通信傍受のためには、裁判官の発する令状が必要であることになった。傍受期間は 4 ヶ月以内であるが、更新請求が可能である。1999 年に、4687 件の請求が行われ、4577 件が発付されている。発付された件数のうち、更新請求以外のものは、2978 件となっている。<br>なお、2000 年 11 月の判決によると、電子的なメッセージは、同国の電気通信法典により保障されており、その傍受は国家の安全保障等の目的が明確に定義された理由に基づく場合以外は違法である。<br>通信傍受の概要は、以下の通りである。<br>・ 対象となる通信手段は、電話，ファックス，コンピュータ通信等の電気通信である<br>・ 対象となる犯罪は、罪又は法定刑が２年以上の拘禁刑の軽罪に該当する刑法の罪である<br>・ 令状発付の要件は、予審手続上必要と認められることである<br>・ 傍受期間は 4 ヶ月以内であるが、何度でも更新請求が可能である<br>・ 令状発付者は、予審判事である<br>・ 傍受の範囲は、傍受の間に行われたすべての通信をであり、操作のために真実発見に有用な通信を反訳することになる<br>・ 予審被告人又は私訴原告人の弁護人は，予審記録を閲覧することができる |

| 国名 | 欧州サイバー犯罪条約データの保全（第 16 条、第 17 条）提出命令（第 18 条）捜索および押収（第 19 条）に係る各国の法律 | | リアルタイム収集（第 20 条）通信傍受（第 21 条） |
|---|---|---|---|
| | 個人 | 通信事業者 | |
| ドイツ | （刑事訴訟法）<br>被疑者については、自己負罪拒否特権を根拠に、提出義務はないという見解が一般的である。 | （電気通信法）<br>1996 年電気通信法第 88 条において、捜査機関による通信傍受のための設備の設置については、事業者の負担によるものと定められた。<br>なお、犯罪捜査のために例外的に長期間、通信履歴の保存を認める旨の規定は見当たらない。<br>プロバイダは、電話番号や住所氏名等の顧客データをデータベースとして維持管理しなければならないことや、これらのデータについて、業者に認識させずに司法当局がアクセスできる環境を確保しなければならないことが規定されている。また、郵政電気通信監督官庁及び安全保障官庁（裁判所・検察庁・警察等）は、電気通信事業者への通知なしに、当該電気通信事業者の有する顧客データを呼び出すことができることとされている。さらに、電気通信事業者は、顧客の承認を条件として、顧客に関するデータの収集・処理・利用を行うことができることが規定されているほか、犯罪の未然の防止又は犯罪捜査のために必要であれば、顧客への通知を行わずに当局に対してデータを開示しなければならないこととされている。<br><br>（刑事訴訟法）<br>また、差押え物一般について、それを所持している者には、捜査機関の要求に応じて、それを提示し、引き渡す義務があり、それを拒絶した場合には、裁判官が、それに対する制裁として、金銭の支払いおよびそれが徴収できない場合の拘禁を命ずることができる。 | （ドイツ基本法）<br>ドイツ基本法により、公権力による通信の秘密の制約としての通信傍受を規定している。<br>1998 年に、捜査機関が一般家屋内部に傍受装置を設置する権限を認める、第 13 条に係る改正がなされた。<br><br>（基本法第 17 補充法、および信書・郵便及び電気通信の秘密に関する法律）<br>公安・予防目的での通信の秘密の制限、刑事訴訟法上の電信・電話の傍受、一般的な関係者の守秘義務や協力義務、について規定されている。<br><br>（犯罪対策法）<br>上記信書・郵便及び電気通信の秘密に関する法律を改正し、通信の秘密の制限を拡張した。<br><br>上記各法を総合し、通信傍受の概要を総括すると、以下の通りである。<br>・ 対象通信手段は、電話，ファックス，コンピュータ通信等の電気通信のほか，非公開の会話を含む<br>・ 対象犯罪は、国家転覆、通貨・有価証券偽造、武器火薬の不法製造、麻薬、外国人法違反等である<br>・ 傍受期間は 3 ヶ月以内であるが、何度でも更新請求可能である<br>・ 令状の発付は、裁判官が行う（ただし、急を要するときは，検事局も発することができるが，この場合，３日以内に裁判官に承認されないときは効力を失う）<br>・ 傍受対象の通信範囲は、傍受の間に行われたすべての通信を記録し，その中で重要な部分を反訳する。傍受の処分により得られた個人関連情報は，その利用の機会に，対象犯罪の犯罪行為の解明のために必要な知識であるときに限り，他の刑事手続における証明目的のために使用することができる。 |
| ロシア | | | （通信法）<br>1995 年に制定された「通信法」により、電話・電子メール・郵便の傍受のためには、裁判所の令状が必要となった。<br>しかし、連邦保安局が 1998 年に発した命令（連邦政府通信・情報局指令第 130 号）においては、プロバイダに対して通信傍受のための装置設置が求められた。この命令に関する裁判の結果、ロシア最高裁は、第 130 号を無効であるとの判断を下している。 |