



犯罪目的の情報通信テクノロジーの使用に対抗するための包括的な国際条約を 作成するための特別委員会

再招集された最終会合 2024年

7月29日～8月9日

国連人権高等弁務官事務所の提出書類

2024年7月22日

I. はじめに

国連人権高等弁務官事務所（OHCHR）は、2024年5月に公表されたサイバー犯罪条約草案の第3次改訂版に対してコメントを提供する機会を歓迎する。[1]

サイバー犯罪が世界中の人々の権利を脅かしていることは否定できない。国連の後援の下、サイバー犯罪条約を締結すれば、犯罪化へのアプローチを統一し、効果的な捜査枠組みを提供し、国境を越えた情報交換を促進することで、刑事免責を減らすことができる。これを実現するためには、合法性、必要性、比例性、適正手続き、法の支配といった原則に沿って、新しい条約を国際人権法にしっかりと根付かせることが不可欠である。これを怠れば、サイバー犯罪に対処する努力が損なわれ、信頼が損なわれ、人権侵害や濫用が助長されることになる。これは、社会の安全性や活力を低下させ、公正さや公平さを低下させる環境を助長することになる。

交渉の当初から、OHCHRは条約の草案について、人権の観点からコメントや具体的な条文の提案を行ってきた。[2]こうした指摘の多くは、多くの加盟国、市民社会組織、民間部門の代表者からも、さまざまな形で提起されてきた。

¹A/AC.291/22/Rev.3.

²https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf,
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_intersessional_consultation/Pres_entations/Panel_1_OHCHR.pdf,
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/AHC4_OHCHR_comments_10_January_2023.pdf,
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/OHCHR_sub_mission_5th_session_Ad_Hoc_Committee_Cybercrime.pdf,
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/OHCHR1.pdf,
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/OHCHR2.pdf を参照のこと。



改正草案には歓迎すべき改善点がいくつか含まれている。しかし OHCHR は、多くの条項が国際人権基準を満たさないという重大な欠点に対して懸念を抱いている。これらの欠点は、表現の自由を不当に制限し、反対意見を標的にし、通信のプライバシーと匿名性を恣意的に妨害するために、一部の法域で既存のサイバー犯罪法がすでに拡大解釈的に使用されていることをえると、特に問題となる。

以下のコメントは、交渉の現段階で特に関連があると思われる**主な分野**に焦点を当てている。条約を採用するために早急に対処しなければならない未解決の問題が数多くあることから、網羅的なものとは理解されるべきではない。

II. 人権の尊重

OHCHR は、条約の解釈と実施における包括的な義務と原則としての人権尊重を強調する**第 6 条と第 24 条**に人権への言及が含まれたことを歓迎する。刑事責任の過大な要求と刑法犯罪の捜査および訴追は、個人に対する国の法的権限の行使の範囲内にあり、したがって国際人権法の下で定められた制約に従う。人権に直接言及することは、刑法犯罪の確立と犯罪の捜査・訴追は、国際協力を通じたものも含め、人権に広くかかわる複雑な問題を提起するという条約の認識を反映したものである。これは、犯罪化規定の過度の広範な実施を避けるための基礎を提供し、法の適正手続きと公正な裁判の保護の完全な尊重を含め、個人の権利に対する恣意的な干渉を防ぐための強固な保護措置を講じる必要性を強調している。この基本的な点は、現行草案の第 6 条 1 項に、**特定の人権文書**、特に市民的及び政治的権利に関する国際規約への**明確な言及**を含めることによって、さらに強化することができる。

OHCHR は草案に**第 6 条 2 項**が追加されたことを全面的に支持する。この条文は、条約が国際人権法の定めを越えて人権を制限することを認めないことを明確に示している。また、この条文は、サイバー犯罪法や手続的措置を利用して人権を不当に制限するという憂慮すべき傾向に対して、重要な追加的保護層を提供するものである。

III. 犯罪化

交渉プロセスの当初から、OHCHR は**この制度における刑法犯罪の範囲を狭く**し、サイバーに依存する刑法犯罪に**限定する**よう勧告してきた。これらの犯罪とは、データやシステムの完全性、機密性、可用性に対する犯罪、このような犯罪を犯す目的でデバイスを悪用した犯罪、コンピュータ詐欺のような限られた特定のコンピュータ関連犯罪など、コンピュータのデータやシステムに本質的に関連する犯罪である。先に述べたように、サイバー犯罪の定義が広すぎる法律は、国際人権法で保護されているオンラインコンテンツに関連する行為を犯罪化するなど、表現の自由に対する権利に不当な制限を課すために頻繁に使用されている。特に、犯罪についての曖昧で漠然とした文言や広範な定義が含まれることによって、狭い範囲を超えて拡大された犯罪の定式化は、将来の人権侵害や虐待のリスクを大きく高めることになるだろう。



こうした背景から、OHCHR は以前から、ヘイトスピーチ、過激主義、テロリズムといった問題に関する広範な規定を含むような犯罪化の範囲拡大の提案に懸念を示しており、それらが現在の草案に含まれていないことを歓迎する。しかし、新たな犯罪に焦点を当てた**選択議定書**の交渉が計画されていることから、このような広範な規定が新たな議定書に盛り込まれる可能性があり、合法性、必要性、比例性という国際人権基準に反する懸念がある。

この文脈で OHCHR は、「国連サイバー犯罪防止条約（情報通信テクノロジー・システムを使用して行われる犯罪）」という**条約の新しいタイトル案**にも懸念を抱いている。これは、ICT システムを通じて行われるあらゆる犯罪行為をサイバー犯罪と定義していると解釈されかねない。このようなアプローチは、この条約の目的を「サイバー犯罪」と闘い、防止することと定義している第 1 条を背景として、特に問題となる。条約の下で刑法犯罪の範囲を明確かつ狭く定義された犯罪に限定しようとする試みに反して、タイトルと合わせて読んだ場合、目的の拡大解釈につながる可能性がある。

OHCHR は、**第 4 条**（旧第 17 条）の無制限な性質に懸念を抱いている。現在、条約草案の中で非常に目立つ位置にある第 4 条は、コンピュータ・システムを使用して犯罪が行われた場合、条約の適用範囲を他の国際文書に基づく犯罪にまで拡大するための措置を採択することを各国に求めている。関連する犯罪の網羅的なリストがないため、この規定の実際の適用範囲は明確ではなく、現時点では将来的な影響を評価することは不可能である。テロの定義が広すぎるなど、他の条約の適用で経験した問題が拡大するリスクもある。また、この規定はサービスプロバイダーに対する不釣り合いな法的義務体制の確立につながりかねず、ひいては表現の自由を脅かすことになる。したがって **OHCHR は、狭い範囲と明確な条約の適用を確保するため、第 4 条の削除を勧告する。**

刑法犯罪は、影響を受ける個人が特定の行為に関して法的義務にさらされることを合理的に予見できるようにし、法の執行における一貫性を確保し、規範を執行する当局の自由裁量を回避するために、合法性の原則が要件となるように、十分な精度をもって策定されなければならない。刑法は、対応策として刑事制裁を必要とする行為のみを対象とし、それ以外の行為が犯罪化されるリスクにさらされないようにすべきである。この点に関して、OHCHR は以前にアドホック委員会に提出したコメントに言及する。[3]

第 7 条から第 12 条について、OHCHR は、この条約の対象となる行為を犯罪化するための前提条件として、「不正の意図」や「犯罪の意図」といった限定的な意図の存在を明示的に含めることを勧告する。 そうすることで、この条約の適用が不透明で広範な行為に及ぶことを防ぐことができる。現在の条約案で使用されている「故意に intentionally」という表現はあいまいなままであり、その行為が有害とはいえ実際には公益と社会全般にとって有益な行為の犯罪化を許してしまう可能性がある。

³https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multistakeholders/OHCHR1.pdf、特に 3-6 ページ。

例えば、サイバーセキュリティの専門家やリサーチャーは、システムの弱点を特定し、セキュリティを強化したり、サイバー犯罪を防止したりすることを目的としているが、コンピュータシステムへの「不正アクセス」に関する第 7 条は、コンピュータシステムの全部または一部への権利のない故意によるアクセスを犯罪とするものである。同条は現在、6 条 1 項における既定の要件としてよりも、6 条 2 項における国家の裁量的な選択肢としてのみ、限定的な意図の基準を定めている。

条文自体の変更合意することが困難であることが判明した場合、特に、必要とされる高い要件を記述する適切な表現を見つけることが困難であることを考えると、解釈上の注釈は、あまり好ましくないとはいえ、追加的な明確性を提供するための代替手段となりうる。

OHCHR はさらに、**オンライン上の子どもの性的虐待または性的搾取の素材に関する** 条文（第 14 条）が、子ども自身が作成したコンテンツを犯罪の対象とすることを適切に防いでいないことを留意する。現行草案の**第 14 条 4 項**は、各国が「子どもたちが自ら作成した素材や」「同意に基づく性的関係の一部として作成された素材に対する犯罪化を排除するための措置を講じることができる」と規定している。この規定のオプション的な性格だけでなく、「措置を講じる」という要素も、この排除を弱め、国際法で求められている子どもの権利の十分な保護を提供していない。OHCHR は、この裁量的なコミットメントは、国際法の下で保証されている子どもの権利の十分な保護を提供しないと考えている⁴。したがって OHCHR は、国際人権法と両立しない場合、子どもによる自己生成物の犯罪化を明確に排除するために、「してもよい」という言葉を「行わなければならない」に置き換えることを勧告する。

第 14 条は、「子どもの性的虐待または子どもの性的搾取の素材」とみなされるコンテンツの種類と範囲、および犯罪化されようとする行為に関して、さらに複雑な疑問を投げかけている。特に、子どもを「表現」しているコンテンツ（**第 14 条 2 項**）の犯罪化には、例えば、架空の人物を描いた芸術や文学の正当な表現や、子どもの性的虐待の事例に関する報道や歴史的研究が含まれる可能性がある。この規定の精度を高めたり、適切な例外を設けることがなければ、この条文はジャーナリスト、科学者、芸術家による不適切な検閲を可能にするリスクをはらむことになる。

OHCHR は、**第 16 条**（親密な画像の非同意的共有）が 18 歳以上の個人にのみ適用されることに留意する（第 16 条(2)）。この制限の背景には、子どもは親密な画像を共有することに同意できないという理由があるように思われるが、OHCHR は、現在の規定が、同意なしに画像が共有される 18 歳未満の個人に対する保護のギャップを残す可能性があることを懸念している。もし彼らが国内法の下で性行為に従事する法定年齢に達しており、かつその画像が子どもの性的虐待や搾取を描いていないのであれば」、第 16 条を 18 歳未満の子どもに拡大することを、単に国の任意とすることによって、この選択肢を使用しない法域の子どもたちは、子どもの性的虐待や搾取に当たらない親密な画像の非同意的な共有に対する保護を欠くことになる。

⁴子どもの権利委員会は、デジタル環境に関連する子どもの権利に関する一般的意見第 25 号（2021 年）（CRC/C/GC/25）において、自己生成物に対する子どもの犯罪化に関して、次のように述べている：「私たちは、子どもたちの同意を得て、子どもたち自身の私的使用のためにのみ、子どもたちが所有および/または共有する、子どもたち自身による性的素材を犯罪化すべきではない。子どもたちが安全にアドバイスや支援を求めることができるよう、子どもにやさしいチャンネルを設けるべきである。（また、「子どもは、サイバー犯罪法を侵害したと主張され、告発され、または認知される可能性がある。締約国は、政策立案者がこのような法律が子どもに及ぼす影響を考慮し、予防に重点を置き、サイバー犯罪に代わる法律を作り、使用するためのあらゆる努力をするよう確保すべきである。刑事司法の対応」（パラ 117）。



この「かもしれない (may) 」という言葉 を 「行わなければならない (shall) 」という言葉に置き換えることで、このギャップを埋めることができるだろう。

OHCHR は **第 18 条** の現行版について懸念を表明したい。これは締約国に対し、「この条約に従った犯罪への参加に対する」法人の法的義務の立証を要件とするものである。第 19 条とは異なり、第 18 条の文言はいかなる故意も要件としていない。この省略は、ユーザーがアップロードまたは共有するコンテンツを含め、ユーザーの行為に対する法的義務をサービスプロバイダに拡大するリスクとなる。この場合、サービスプロバイダーは法的義務を回避するために、プラットフォームやサービス上のすべての通信やデータのスキャンやフィルタリングなど、厳格な措置を実施せざるを得なくなる。このアプローチは、大規模なプライバシー権への不当な干渉につながり、人権によって保護される膨大なコンテンツの削除やブロックを促すことになる。こうした**重大なリスクを防ぐため、OHCHR は 第 18 条 1 項を改正し、意図的に明確な要件を盛り込むよう勧告する**。第 18 条 1 項は以下のように改正されることになる。

「各締約国は、この条約に従って定めるものに対する法人の参加責任を確立するために、**当該法人が、その実行された特定の犯罪について少なくとも実際の知識を有していた場合には、** 自国の法原則に照らして必要とされる措置を採用するものとする」。

IV. 手続き上の措置と条件、セーフガード

監視やデータの収集に関するものなど、サイバー犯罪の捜査に関連するいくつかの手続き上の措置は、その性質上、プライバシー権やその他の権利に特に干渉するものであり、悪用や濫用を防止するための条件や保護措置の強固な枠組みが必要である。この点で、条約草案には大きな欠点がある。

第 4 章（手続上の措置および法の執行）の**範囲が広く**、デジタル痕跡を残す可能性のあるあらゆる犯罪を実質的に対象としている（第 23 条 (2)(b)(c) 参照）ことは、懸念の理由となる。OHCHR は、手続的措置の範囲を第 2 章で定められた刑法犯罪の捜査に限定することを勧告する。それにもかかわらず、手続的措置の範囲を条約で定める犯罪よりも広くすることが決定された場合、OHCHR は、手続的措置の範囲を「重大な犯罪」に限定することを勧告する。この犯罪は、少なくとも 4 年の自由の剥奪という刑罰が要請国と被要請国の双方で適用される犯罪と定義され、死亡または身体的危害、明確に定義された金融犯罪、暴力行為の強要など、犯罪に「有害性」という質的要素が追加的に適用される。

さらに、条約草案 **第 23 条は**、コンテンツデータの傍受を除くすべての手続的措置は、問題の犯罪の性質や重大性に関係なく、あらゆる種類の犯罪を捜査するために利用できると定めている。たとえば、条約の下でのコンピューターやデータの検索・押収の規定は、「不敬罪」や「国家に対するプロパガンダ」とみなされる可能性のある芸術表現について、実際には人権法の下で正当な表現であるにもかかわらず、適用される可能性がある。これは、人権を尊重する義務や、一般的な法執行措置に適用可能な必要性と比例性の原則と、実際には両立させるのが難しい。



OHCHR はさらに、手続き上の措置が、(i)刑法犯罪が行われた、または行われると信じるに足る合理的な理由がある、(ii)その措置によって犯罪に関する関連情報が得られる可能性が高い、という場合にのみ適用されることを保証する明確な文言が、**第 23 条と第 24 条**にないことを懸念している。これは、国際人権法上正当な理由なく権利を制限する措置を可能にするリスクとなる。「適用を正当化する理由」という表現は、これらの要件をカバーするように解釈できるかもしれないが、明確性と具体性に欠ける。

一般的に、第 24 条は、考えられる条件やセーフガードを列挙するだけで、それらをいつ、どのように適用するかは締約国の裁量に委ねられており、**人権に基づく強固な拘束力のあるガードレール体制を確立していない**。合法性と必要性の原則、権限を行使する際の事前の司法その他の独立した承認、影響を受ける個人および団体に対する十分な通知その他の透明性措置、弁護士とクライアントの通信を含む秘匿特権通信の秘密保持の尊重⁵への言及が完全に欠落している。

前述の段落で提起された懸念に対処する規定として、国内手続き上の措置と国際協力の双方を対象として、次のような規定が考えられる：

1. この条約に基づく権限および手続を確立し、実施し、適用する義務は、この条約が定める特定の刑法犯罪の捜査に必要な限りにおいてのみ適用される。
2. 締約国は、このような権限及び手続が、条約が定める犯罪が行われ、又は行われることが予見されると信じるに足る理由を与える事実的根拠があり、かつ、その措置を通じて犯罪に関する関連情報が得られる場合にのみ実行されることを確保する。
3. これらの権利および手続は、国際人権法に基づく締約国の義務に従い、実効的な条件および保障措置に従うものとする。かかる条件および保障措置は、とりわけ、合法性、必要性および比例性の原則を組み入れ、かかる権限の行使について事前の司法またはその他の独立した承認およびレビューを定め、かかる権限または手続の範囲および期間の制限を定め、影響を受ける個人および団体に対する十分な通知およびその他の透明性措置を定め、かかる権限または手続行使の結果として損害を被る個人に対する効果的な救済へのアクセスを定め、弁護士-依頼者間およびその他の秘匿特権通信の秘密を尊重するものとする。
4. この条約に基づく権限および手続の秘密は、サービスプロバイダに課される場合を含め、問題となっている特定の犯罪の効果的な捜査を可能にするために必要な期間および範囲に限定されるものとする。問題となっている権限および措置の影響を受けるすべての者は、速やかに通知されるものとする。

⁵犯罪の防止と犯罪者の処遇に関する第 8 回国連会議が 9 月 7 日に採択した「[弁護士](#)の役割に関する基本原則」第 22 原則参照。弁護士とクライアントの関係における守秘義務の保護については、「[裁判官と弁護士の独立に関する特別報告者報告書](#)」[A/71/348](#)、パラ 45-49 を参照のこと。



ただし、このような通知は、特定の犯罪の効果的な捜査を妨げてはならない。

具体的な措置に関して、OHCHRは**第29条**（トラフィックデータのリアルタイム収集）と**第30条**（コンテンツデータの傍受）の削除を勧告する。その非常に侵襲的な性質と潜在的な範囲の広さから、このような措置はほとんどの刑法犯罪と闘うには不釣り合いである可能性が高い。重大でない犯罪にまで及ぶ広範な刑法犯罪に対して、また、その合法性、必要性、比例性を評価できる事前の司法承認という明確な要件なしに、このような措置を実施する義務を条約に課すことは、大規模なデータ収集を含め、プライバシー権への恣意的な干渉による誤用や乱用の大きなリスクをもたらすだろう。この懸念は、多くの国の国内的枠組みや制度的能力がこうしたリスクを防止・軽減する準備を整えていない可能性がある現状によって、さらに悪化している。

OHCHRはまた、人権の効果的な保護に対して特にリスクを伴う**第28条（4）**（保存データの検索と押収）の削除も勧告する。例えば、この条項により、国家は第三者に対し、特定のソフトウェアの脆弱性を開示するよう強制することができる。同様に、国は復号化、暗号鍵の開示や復号化における積極的な支援の提供を強制することができる。命令は、問題となっているICTシステムの運用者だけでなく、その運用者の従業員を含むあらゆる者を対象とすることができる。要求される手段は、通信内容の改ざんを可能にする可能性さえある。

そのため、第28条4項は、複数の裁判管轄権を有する場合を含め、さまざまな種類の通信の監視を可能にし、通信の秘密と安全に対する不当な干渉につながる可能性がある。さらに、第28条4項で提案されているように、当局はサードパーティに対してアクセスを強制することが許されるのであれば、そのようなアクセスは、司法の承認を要件とすることなく、監視のような、より広範で関連性のない目的にも容易に適用することができる。さらに、想定されるセキュリティギャップを埋めることなくソフトウェアの脆弱性を特定することは、通信における既存のセキュリティ基準を危うくし、結果としてサイバー犯罪の実行を助長する可能性がある。

V. 国際協力

現在の国際協力の広範な範囲も、人権問題に一連の懸念を生じさせる。現在議論されている草案は、たとえそのような行為の犯罪化が国際人権基準に反するものであったとしても、一部の国によって犯罪と認定されているような例外的な範囲にある行為に関しても国際協力を促し、おそらくは要件とさえするだろう。このような結果を避けるため、OHCHRは国際協力の目的を**狭い範囲**に限定することを勧告する。言い換えれば、国際協力に関する規定は、条約自体によって定められた刑法犯罪にのみ関係するものとするを勧告する。

国際協力の範囲が上述の勧告以上に拡大される決定がなされた場合、OHCHRは、国際協力が最低限、「**重大な刑法犯罪**」に限定され、**要請国と被要請国の両方において**少なくとも4年の自由剥奪が適用されるという要件によって定義されることを勧告する。



私たちは、犯罪に適用される**有害性の質的要素をさらに追加**する。たとえば、死亡または身体的危害、明確に定義された金融犯罪、強制的行為の強要などである。このような制限を設けることで、国際協力の枠組みがより明確になり、潜在的な悪用のリスクを軽減しつつ、要請された国の能力を圧迫することなく、各国が有意義な協力を行えるようになる。この文脈において、第 35 条 1 項 (c) の「この条約の適用を採択するために～重大な犯罪を含む、」の文言は余計であり、削除されるべきであることにも留意すべきである。

(c) ~~この条約の適用を採択するために効力を有する他の適用可能な国際連合条約及び議定書に従って成立した重大な犯罪を含む、あらゆる重大な犯罪に関する電子形式の証拠の収集、入手、保全及び共有。~~

さらに、この条約が協力と相互法的支援のために**適切な範囲の条件と保障措置**を採択することが最も重要である。明確に定義された条件や保障措置がなければ、人権上の権利に抵触し、保護格差が生じ、政府の行き過ぎた行為を助長する可能性が高い。最終的な条約は、少なくとも法の執行と手続き上の措置に関する章で規定されているレベルの国際協力に関する条件と保障措置を規定することが不可欠である。このような背景から、OHCHR は、第 24 条の適用を協力シナリオにまで拡大する**第 23 条 4 項**が盛り込まれたことを歓迎する。しかし、このようにして確立された枠組みは、まだ明確性と具体性を欠いている。OHCHR が提案する**一般的なセーフガード**条項は、第 4 章のセクションで述べたとおり、より強力な人権保護の枠組みを保証するものである。

条約が犯罪と闘うための効果的な協力の基礎となり、特に政治的な目的のために国家による人権侵害の越権行為を助長しないようにするためには、協力**拒否の強力な強制的根拠**を規定することが不可欠である。条約には、国際協力と相互法的支援を拒否する根拠として、少なくとも以下の 3 つを盛り込むものとする。

- 双罰性がない場合、言い換えれば、すべての協力国が国際協力と法的共助の対象となる行為を犯罪化しているわけではない場合
- 国際協力および法的支援の要請が政治犯罪に関するものである場合
- 援助が、国際人権法で禁止されている差別を含むが、これに限定されない人権の侵害や濫用につながる可能性があるると合理的に考えられる場合

こうした背景から、OHCHR は、差別の禁止事由に基づく訴追や処罰を対象とする**第 40 条 22 項**が盛り込まれたことを歓迎する。拒否の根拠は、人権侵害をより広くカバーするよう拡大されるべきであり、国際人権法の下での尊重と保護の義務の表現として義務化されるべきである。そのために、OHCHR は以下の文言を提案し、**新たなパラグラフ 21bis**を導入し、**パラグラフ 22**を修正する。

21bis. 相互法的援助は、以下の場合には、拒否されるものとする。(a) 刑法犯罪が要請国によって政治犯罪として取り扱われると信じるに足りる合理的な理由がある場合



(c) 要請された締約国の当局は、何らかの類似の犯罪に関して要請された行為を実施することが国内法によって禁止されている場合であって、自国の司法権の下で捜査、訴追その他の手続の対象となっていた場合

22. この条約のいかなる規定も、相互の法律扶助を与える義務を課すものと解釈してはならない。要請された締約国が、要請が、その者の性別、人種、言語、宗教、国籍、民族的出身若しくは政治的意見を理由としてその者を訴追し若しくは処罰することを目的として行われたものであると信ずるに足りる相当な理由がある場合又は要請に応ずることがこれらの理由のいずれかによりその者の地位を害することになると信ずるに足りる相当な理由がある場合には、相互の法律扶助は拒絶される。

VI. 結論

最終会期は、デジタル時代の人権にとって極めて重要な時である。サイバー犯罪に取り組み、犯罪捜査における国際協力を可能にすることは、人権の擁護と前進と両立させられなければならない。OHCHR はすべての交渉当事国に対し、国際法、基準、原則を厳守しつつ、新条約が全条文を通じて人権を包括的に統合するよう、あらゆる努力を払うよう求める。このような統合が達成されなければ、世界の人々の人権保護が危うくなり、インターネット・インフラの機能が損なわれ、新たな安全保障リスクが生じ、ビジネスチャンスや経済的福祉が損なわれる可能性がある。

OHCHR はこの機会に、国際人権基準に沿ってサイバー犯罪に対処するという約束を包括的に実現できる新しいサイバー犯罪条約の起草と、採択された場合にはその実施において、加盟国、特に特別委員会の会期に参加する代表団を支援するという約束を再確認する。

本文提案の要約

タイトル

国連サイバー犯罪防止条約（情報通信テクノロジー・システムを利用して行われる犯罪）

第2条

「重大な犯罪」とは、**要請国及び被要請国の双方において、最高4年の自由剥奪又はこれより重い刑罰により処罰される犯罪を構成する行為であって、死刑又は身体的危害、金融犯罪若しくは強制行為を伴うものをいう**；

第4条

削除。

条件と保護措置に関する一般規定

1. この条約に基づく権限および手続を確立し、実施し、適用する義務は、この条約が定める特定の刑法犯罪の捜査に必要な限りにおいてのみ適用される。
2. 締約国は、このような権限及び手続が、条約が定める犯罪が行われ、又は行われる予定であると信じるに足りる理由を与える事実に根拠があり、かつ、その措置を通じて犯罪に関する関連情報が得られる場合にのみ実行されることを確保する。
3. これらの権利および手続は、国際人権法に基づく締約国の義務に従い、実効的な条件および保障措置に従うものとする。かかる条件および保障措置は、とりわけ、合法性、必要性および比例性の原則を組み入れ、かかる権限の行使について事前の司法またはその他の独立した承認およびレビューを定め、かかる権限または手続の範囲および期間の制限を定め、影響を受ける個人および団体に対する十分な通知およびその他の透明性措置を定め、かかる権限または手続の行使の結果として損害を被る個人に対する効果的な救済へのアクセスを定め、弁護士-依頼者間およびその他の秘匿特権通信の秘密を尊重するものとする。
4. この条約に基づく権限及び手続の秘密は、サービスプロバイダに課される場合を含め、問題となっている特定の犯罪の効果的な捜査を可能にするために必要な期間及び範囲に限定されるものとする。問題となっている権限および措置の影響を受けるすべての者は、そのような通告が特定の犯罪の効果的な捜査を妨げない限り、速やかに通告されるものとする。

第7条

1. 各締約国は、次のような立法その他の措置を採用するものとする。**不正または犯罪の意図をもって故意に行われた場合に、情報通信テクノロジー・システムの全部または一部への権利なきアクセスを国内法の犯罪として確立することが必要である。**



2. 締約国は、セキュリティ措置を侵害すること、電子データの入手その他の不正もしくは刑法犯罪を犯すことを故意にすること、または他の情報通信テクノロジー・システムに接続されている情報通信テクノロジー・システムに関連して犯罪を犯すことを要件とすることができる。

第 8 条から第 10 条、第 12 条についても同様の変更を加えるべきである。

第 14 条 2 項に続く新たなパラグラフ

芸術的、教育的、科学的な性格が明白で、18 歳未満の者が関与しない素材は、第 13 条第 1 項の適用を免除される。

第 14 条 4 項

4. 締約国は、以下の犯罪化を排除するための措置をとることができる：
- (a) 本条第 2 項に記載されている、子どもを描いた自作素材に対する子どもの行為
 - (b) 本条第 2 項(a)から(c)に記載された資料に関する本条第 1 項に定める行為であって、当該資料が、国内法によって決定され、適用可能な国際的義務に合致するように、同意に基づく性的関係の一部として作成され、かつ、関係者の私的かつ同意に基づく使用のためにのみ保持されるものである場合。

第 16 条 3 項

3. 締約国は、国内法の下で性行為を行うことができる法定年齢に達しており、かつ、その画像が子どもの虐待又は搾取を描いていない場合には、適宜、親密な画像の定義を 18 歳未満の者の描写に拡大することができる。

第 18 条 1 項

各締約国は、この条約に従って定めるものに対する法人の参加責任を確立するために、その**犯された特定の犯罪について法人が少なくとも実際に知っていた場合には**、自国の法原則に合致する必要な措置を採用するものとする。

第 23 条 2 項

2. この条約に別段の定めがある場合を除くほか、各締約国は、この条第一項にいう権限及び手続を次の各号に適用する。

- (a) この条約に従って定められた刑法犯罪；
- (b) 情報通信テクノロジー・システムを利用して行われた、**重大な刑法犯罪とみなされる**その他の犯罪、
- (c) **この条約に従って成立した刑法犯罪または重大な刑法犯罪の証拠**を電子的な形式で収集すること。

第 28 条 4 項

削除

第 29 条 および 第 30 条

削除

第 35 条 第 1 項(c)

(c) この条約の適用を採択するために効力を有する他の適用可能な国際連合条約及び議定書に従って成立した重大な犯罪を含む、重大な犯罪に関する電子形式の証拠の収集、入手、保全及び共有。

第 40 条(21 の 2) および 第 22 条

21bis. 相互法的援助は、以下の場合には、拒否されるものとする。(a) 刑法犯罪が要請国によって政治犯罪として取り扱われると信じるに足りる合理的な理由がある場合 (b) 協力又は援助が人権侵害をもたらすと信じるに足りる合理的な理由がある場合、(c) 要請された締約国の当局は、何らかの類似の犯罪に関して要請された行為を実施することが国内法によって禁止されている場合であって、自国の司法権の下で捜査、訴追その他の手続の対象となっていた場合には、拒否される。

22. この条約のいかなる規定も、相互の法律扶助を与える義務を課すものと解釈してはならない。要請された締約国が、要請が、その者の性別、人種、言語、宗教、国籍、民族的出身若しくは政治的意見を理由としてその者を訴追し若しくは処罰することを目的として行われたものであると信ずるに足りる相当な理由がある場合又は要請に応ずることがこれらの理由のいずれかによりその者の地位を害することになると信ずるに足りる相当な理由がある場合には、相互の法律扶助は**拒絶される**。