第１４０回国際研修
平成２０年９月１日（月）から同年１０月１０日（金）まで

１　研修の主要課題は，「サイバー犯罪に対する刑事司法による対応」です。

（１）サイバー犯罪の脅威の増大と対策の必要性

情報通信技術の発展は，社会及び人々の生活を急激かつ根本的に変えつつあります。情報通信技術，特にコンピュータとそのネットワークは，様々な社会的・経済的活動の管理・伝達手段として，今や更なる発展のために欠かせない存在とみられるようになりました。

その一方，遺憾ながら，コンピュータとそのネットワークは，これを対象とし（不正アクセス，コンピュータデータ又はプログラムの毀損・変更等）又はこれを手段とする（詐欺，偽造，児童ポルノ，名誉毀損，知的財産権侵害等）様々な犯罪を生むに至りました。情報通信技術の進展は，悪戯心から他人のコンピュータへ侵入しようとする者に自己満足の機会を与えるだけでなく，組織犯罪グループに個人情報盗用，偽造クレジットカード詐欺，不法取引[※1]等で経済的利益を得させることも容易にしています。情報通信技術を利用した個人情報に関わる不正行為，例えばコンピュータ侵入，フィッシング，スキミング等は，他人のプライバシーを侵害するだけでなく，これを利用した経済犯罪の手段ともなっています。児童ポルノ，著作権侵害のほか，暴力・薬物・経済・性犯罪，自殺，テロを助長するウェブサイトなど，様々な違法有害情報も容易に閲覧可能です。社会生活基盤に対するサイバー攻撃は，即座に国内外の社会・経済システムにも深刻な影響を及ぼし得ます。このように，サイバー犯罪は，様々な形で社会全体や人々の権利，特に財産，尊厳，場合によっては生命まで脅かすようになっています。

このような状況に対処するには，サイバー犯罪（この研修では，コンピュータ及びそのネットワークが対象又は手段となっている犯罪をいいます。）のいくつかの特徴に留意する必要があります。捜査官は，不可視・無形・可変の情報と最先端の技術，広域ネットワークを用いて敢行されるサイバー犯罪に対し，しばしば追跡上の困難に直面することになります。インターネット上の匿名性は，犯罪のための便利な道具となり得ます。サイバー犯罪者は，地域的・時間的制約を受けることもなく，低いリスクで瞬時に広く大衆に害悪を及ぼし得ます。模倣犯もしばしば現れます。

このような現象は先進国において顕著な問題を投げかけていますが，発展途上国にも重大な暗示を与えるものです。サイバー犯罪は，最小限の通信技術さえあれば，これを取り締まる法的枠組みと法執行機関が極めて弱い法域を発信地又は経由地

※1　例えば，西アフリカの国際組織犯罪に関する国連薬物・犯罪事務所のある調査は，Ｅメールが今や時間・距離に関わりなく犯罪集団が意思伝達する手段として欠かせないものとなっており，不正取引の危険が大幅に増大していると指摘しています。

として敢行され得ます※2。情報通信技術が導入・維持されてまもない国は予期せぬ脅威に直面しかねません。社会のさらなる発展のために情報通信技術を最大限活用する上で，サイバー犯罪に対する適切な防御策を構築することは避けられない課題です。

サイバー犯罪が個々の国の健全な発展や国際社会にもたらす脅威は，過小評価されてきました。しかしながら，情報通信技術を利用した犯罪が世界規模で瞬時に莫大な損害をもたらすことに鑑みれば，刑事司法機関がサイバー犯罪に対して直ちに適切な対応をとることは必要不可欠です。それにもかかわらず，多くの国にとってこの種の犯罪は比較的新しく，すべての国が必要な法制度を整備しているわけではありません。仮にそのような法制度が整備されているところでも，刑事司法関係者のサイバー犯罪に対する知識不足と技術的問題が相まって，このような犯罪の捜査，訴追及び公判，特に犯人の特定と証拠の収集において困難が生じます。これに加え，サイバー犯罪特有の複雑な課題に対処するには国際協力も重要であり，究極的には各国が法的，手続的及び規制的な手段をとることが必要となります。

したがって，サイバー犯罪に対する適切な予防・規制策ができる限り速やかに導入されなければなりません。最終的には，刑事司法機関がサイバー犯罪の現況を完全に理解した上，これに対応する適切な法制度を整備し，かかる犯罪の特質に応じた先進技術・手段を開発し，関係する国際協力を促進することが必要になります。

（２）サイバー犯罪対策の国際的取組み

ボーダーレスというサイバー犯罪の特徴に鑑み，様々なレベルでこの問題に対処するための国際的な統合又は協力の取組みがなされてきました。国際レベルでは，国連薬物・犯罪事務所（ＵＮＯＤＣ），国際刑事警察機構（インターポール），主要８か国首脳会議（Ｇ８），欧州連合（ＥＵ），欧州評議会（ＣＥ），米州機構（ＯＡＳ），アジア太平洋経済協力会議（ＡＰＥＣ）など多くの国際機関が，国際協力促進のために必要な政治的・技術的な専門知識を提供してきました。

ア　国連の取組み

国連は，１９９０年の第８回国連犯罪防止会議（コングレス）を手始めに，コンピュータの発展に伴う問題に対応すべく多くの視点から積極的に取り組んできました。１９９４年，コンピュータ関連犯罪の予防・規制に関する国連マニュアルが発刊されました。２０００年の第１０回コングレスでは，国連アジア極東犯罪防止研修所（アジ研）が，コンピュータ・ネットワーク関連犯罪に関するワークショップの企画・実施を支援しました。国連総会は，情報技術の犯罪的濫用との戦いに関する総会決議55/63（２０００年），56/121（２００１年）において，各国政府に対し，情報技術を濫用した犯罪との戦いに際し，各決議の中で列挙された各種対策を考慮するよう示唆しました。２００３年に発

※2　西アフリカを発信源とする悪名高い振り込め詐欺（４１９スキャム）も一例です。

効した国連国際組織犯罪防止条約も，組織犯罪集団によって敢行されるサイバー犯罪について間接的に扱っています。第１１回コングレス（２００５年）においてもコンピュータ関連犯罪に関するワークショップが開催され，ハイテク・コンピュータ関連犯罪を防止，捜査，訴追するための既存の協力の強化，補強に向けた努力を歓迎し，犯罪防止刑事司法委員会（コミッション）に対し，他の機関と連携して，国連の支援の下で一層の支援を提供することの実現可能性について精査することを求めるとの内容を含む「バンコク宣言」を採択しました。２００７年の第１６回コミッションでは，個人情報に関する犯罪についても論議されました。

イ　その他の国際機関における取組み

１９９７年，Ｇ８は，国際組織犯罪対策のための専門家会合であるリヨン・グループの枠組みの下，ハイテク犯罪サブグループを設立し，また，かかる犯罪者にとっての安住の地（セイフ・ヘイブン）を世界からなくすことを目的として，コンピュータ犯罪と戦うための１０の原則を採択しました。Ｇ８ハイテク犯罪サブグループは，ハイテク・コンピュータ関連犯罪について，２４時間体制国際コンタクトポイント（週７日２４時間アクセス可能なコンピュータ犯罪チームのリスト）を創設・拡大しています。

欧州評議会は２００１年１月，欧州評議会サイバー犯罪条約（以下単に「サイバー犯罪条約」といいます。）を加盟国及び招請された非加盟国に対して署名開放しました。２００４年に発効した同条約は，今のところこの分野に関する唯一の拘束力ある国際条約であり，締約国間の国際協力の枠組みを作るとともに，サイバー犯罪に対する包括的な国内法制を整備しようとするその他の国々のガイドラインともなっています。同条約は，締約国に対し，実質的な犯罪行為を定める国内法を一致させるよう求めています。これらの中には，（ア）コンピュータデータ及びシステムの機密性,完全性及び可用性に対する犯罪(不正アクセス・不正傍受・データ妨害・システム妨害・装置の濫用）のほか，（イ）電磁的記録不正作出，電子計算機使用詐欺，（ウ）コンテンツ関連犯罪（児童ポルノ），（エ）著作権侵害関連犯罪が含まれています。２００４年，コンピュータシステムを利用した人種差別的・排外主義的行為の犯罪化に関する同条約の議定書が発効しました。これらに加え，同条約は，提出命令，保全命令，蔵置されたコンピュータデータの捜索・差押え，コンピュータデータの同時収集に関する規定を含む重要な手続的整備を求めています。さらに，同条約は，捜査共助，週７日２４時間体制のネットワーク，犯罪人引渡し等を含む迅速かつ効果的な国際協力システムを構築するための規定も有しています。

２００２年１０月，英連邦諸国の法務大臣らは，サイバー犯罪条約と基本的枠組みを同じくする「コンピュータ及びコンピュータ関連に関するモデル法」を採択しました。２００４年，第５回米州司法大臣・検事総長会合は米州機構

の加盟国に対し，サイバー犯罪条約に示された原則が参考となるか評価し，これに従うことができるか考慮するよう勧告しました。２００５年，第６回アジア太平洋経済協力会議（ＡＰＥＣ）情報通信産業担当大臣会議は，すべての加盟地域に対し，サイバー犯罪条約を研究し，国連総会決議やサイバー犯罪条約を含む国際的な法ツールと整合性を持つようなサイバーセキュリティ及びサイバー犯罪に関する包括的な法制度の策定を模索するよう提言しました。インターポールは，法執行機関のために年中無休ネットワークを含むサイバー犯罪の探知，捜査及び証拠の収集に関する技術援助を行ってきましたが※3，第７回国際サイバー犯罪会議においてサイバー犯罪条約を法的・手続的な国際基準を示すものと評価しました。

それぞれの国においてサイバー犯罪に対する法制度を強化する方策を検討しようとする刑事司法関係者や立法担当者にとっては，以上のようなガイドライン，法的・技術的マニュアルやモデル法制，特にサイバー犯罪条約といった国際的研究の成果資料を評価することが相当といえます。

この研修においては，まず犯罪化については，サイバー犯罪条約及びその追加議定書に規定されているサイバー犯罪を議論の出発点として扱うこととします。しかしながら，その他にもコンピュータやそのネットワークを対象又は手段とする違法又は有害な活動は数多く存在します。その中には，情報通信技術を利用した数々の詐欺的活動，オークション詐欺，インターネット取引詐欺，クレジットカード・デビットカード詐欺などが含まれます。本研修は，このような情報通信技術を対象とし又は他の犯罪の手段として利用するその他のサイバー犯罪をも対象とし得るものとします。

（３）サイバー犯罪の捜査，訴追及び裁判のための法制度的・実務的な課題

いうまでもなく，サイバー犯罪との戦いにおいては，その捜査のために取り得る法的手段及び執行機関の能力を強化することが必須の課題です。しかしながら，犯罪者を適切に処罰してオンライン環境の安全に対する信頼を増すためには，かかる事件を訴追する検察官や審理する裁判官が現状と課題を認識することも重要です。

捜査段階では，捜査の端緒情報を収集する仕組みの強化が考慮されなければなりません。サイバー犯罪の被害者はしばしば被害の届出先やその方法に戸惑うことがあります。児童ポルノなどのコンテンツに関わるサイバー犯罪の被害者は，通常，自ら被害事実自体を届け出る機会すらありません。電磁的証拠は物的証拠に比して消去・破壊が容易であるため，端緒情報を収集した後は，発信源・経路を追跡し，犯人を特定し，証拠を保全・収集するための適時・適切な対応が不可欠です。これを効果的に行うには，捜査官自身が様々な種類のサイバー犯罪及び

※3　例えば，情報技術犯罪に関する欧州ワーキングパーティはサイバー犯罪捜査の技術支援のためのマニュアルを作成しています。

関連する技術に精通するとともに，政府としてもサイバー犯罪捜査機関の能力向上のための方策を講ずることが求められます。プロバイダを含む関係私的団体や技術専門家から必要な協力が得られなければ，時機に遅れることなく適切に無形・可変の電磁的証拠を収集・分析することは困難です。このような場合，捜査機関が蔵置されたコンピュータデータ（通信記録又はコンテンツデータ）又は現に通信中のコンピュータデータを保存，収集及び分析するための強制処分の可否，種類，方法及び程度が最も重要な課題となり得ます。この問題は，大量のコンピュータデータ，想定外のコンピュータデータ，暗号化されたコンピュータデータに対する強制処分についての令状の要否，対象，範囲及び種類といった問題も含みます。その一方，このような電磁的証拠の収集に当たっては，このような捜査はしばしばプライバシーや他の基本的人権と対立し得ることにかんがみれば，適正手続が保障されなければなりません。情報収集及びその後の保存については様々な関係者の利害が対立するため，種々の法的利益の調和点を探求することが求められます。

その上，サイバー犯罪は，管轄と主権を容易に越え得ます。このような場合，捜査を成功に導くためには，異なる法域の捜査機関の間での速やかな情報共有と相互協力を含む国際協力を活用することが必要です。通常の二国間の捜査協力方法では，多くの法域を経由するサイバー犯罪の追跡にとっては不十分です。相当重大なサイバー犯罪については，犯罪人引渡しすら考慮されるべきですが，その場合には双罰性等の問題も生じ得ます。国際協力をより効果的に機能させるためには，一国における実体法上の犯罪と手続法上の手段が他国のそれらと矛盾のないものであった方が望ましいです。その意味でも，サイバー犯罪条約中の手続法と国際協力に関する各条項を検討する意義があるといえます。

訴追段階でも，特に検察官が有体物を想定した規定を無形・短命の電磁情報に適用しようとする際に，実体法・手続法上の様々な問題が生じ得ます。検察官は，訴追の当否と被告人の選択において，慎重に法解釈を検討しなければなりません。

公判段階では，手続法と電磁的証拠の調和の問題が生じ得ます。証拠能力について厳格なルールが求められる法域は勿論，そこまで明確なルールがない法域であっても，裁判官又は事実認定者が無形のデータ証拠を調べることの可否及び方法が問題となり得ます。大量の証拠が関わるサイバー犯罪も実務家に新たな問題を投げかけ得ます。サイバー犯罪も通常は犯意を要件とするところ，犯意の立証方法は法域によって異なるでしょう。このような犯罪は裁判官にとっても比較的新しいため，サイバー犯罪者の適切な処罰のためには，他の法域における量刑の傾向と加重・減軽要素を知ることも有益です。

我々は，本研修において，サイバー犯罪に対する以上のような法制度的・実務的な課題とこれに対処する効果的な対策を探求しようとするものです。

（４）検討事項

この研修の具体的な検討事項は以下のとおりです。

ア　情報通信技術（ＩＣＴ）の分野における違法有害な活動の現状と問題点，特に下記のサイバー犯罪（コンピュータ及びそのネットワークを対象又は手段とする犯罪）の犯罪化について

（ｱ）　欧州評議会サイバー犯罪条約及びその追加議定書に規定された犯罪

- コンピュータデータ及びシステムの機密性・完全性及び可用性に対する犯罪（不正アクセス・不正傍受・データ妨害・システム妨害・装置の濫用）
- 電磁的記録不正作出，電子計算機使用詐欺
- コンテンツ関連犯罪（児童ポルノ，人種差別・排外主義的思想に関連する犯罪）
- 著作権及び関連諸権利の侵害に関連する犯罪

（ｲ）　コンピュータ又はそのネットワークが対象又は手段となっているその他の犯罪（個人情報関連犯罪，インターネットを利用した詐欺，Ｅメールやウェブサイトを利用した暴力犯罪，性犯罪，経済犯罪又は薬物犯罪，名誉毀損等）

イ　サイバー犯罪の捜査・訴追及び公判に関する法制度的・実務的な課題と対策

（ｱ）　捜査上の問題点

a)　捜査の端緒（報告制度，サイバーパトロール等）

b)　犯人の追跡・特定（他の公的・私的機関との連携，２４時間ネットワークの構築等）

c)　証拠の収集・保存（コンピュータデータ（大量のデータ，想定外かつ関連するデータ，暗号化されたデータ等）の適時適切な捜索・差押え，データの保存，提出又は回復，通信記録のリアルタイム収集，コンテントデータの通信傍受等）

d)　電磁的証拠の専門的解析（専門チーム，専門家捜査官等）

e)　国際協力（捜査共助，共同捜査，24/7（年中無休）コンタクトポイントネットワーク，犯罪人引渡し等）

（ｲ）　訴追上の問題点（訴追の可否，管轄及び客体に関わる判断要素，管轄権）

（ｳ）　公判・裁判・量刑上の問題点

a)　証拠法上の問題（証拠能力，大量又は暗号化された証拠の扱い，専門家証人等）

b)　犯意の証明

c)　適正な量刑の手法と要素

2　客員専門家（肩書きは講義当時のもの）

（１）マルコ・ゲルケ氏 (Dr. Marco Gercke)

ドイツ　欧州評議会サイバー犯罪問題顧問，ケルン大学講師

（２）ジョエル・シュワルツ氏 (Mr. Joel Michael Schwarz)

アメリカ合衆国　司法省刑事局コンピュータ犯罪知的財産課　局付検事

（３）ジャン・ユンシク氏 (Mr. JANG Yunsik)

大韓民国　警察大学校教授（警監）