サイバー攻撃に対する国際社会と日本の取組

1　サイバー犯罪条約(ブダペスト条約)

（1）概要

情報技術分野の急速な発達やコンピュータ・ネットワークの発展によって、電子メールの利用、各種サイトへのアクセス、電子商取引等が国境を越えて可能となった。このような情報技術の発展は、社会の一層の発展のため大いなる可能性を秘めているが、他方で、コンピュータ・システムやネットワークを攻撃するような犯罪及びこれらを利用して敢行される犯罪が増加するようになった。

サイバー攻撃は、犯罪となるものも含め、その特性から国境を越えしかも密かに被害を及ぼし得るため、その防止及び抑制のためには緊密な国際的協調のもとに迅速かつ的確な情報共有等の措置をとる必要性が高く、取り分け犯罪として**立件するには証拠保全や適正手続の確保のために法的拘束力のある国際文書が必須**であるとの共通認識が欧州評議会でもたれるようになった。

その結果、欧州評議会は、サイバー犯罪の専門家を召集しプロジェクト会議を設置し、1997年から日米欧を中心に条約策定作業を実施した。そして、2001年11月8日、欧州評議会閣僚委員会において条約文が採択され、**同月23日**にハンガリー、ブダペストにおいて**署名式典**が開催された。我が国も同日署名し、2011年11月23日に10年記念会議が開催。

この条約は、

①コンピュータ・システムに対する違法なアクセス等の行為を犯罪とする(実定法制定)、

②コンピュータ・データの迅速な保全、捜索、押収等の刑事手続を整備する、

③これらの犯罪の犯罪人引渡し等の国際協力を促進する

ことを内容とし、④各国は、一部の規定につき留保を付することを認めている。

（2）現状

2004年7月発効済み。現在の締約国は、米国、英国、ドイツ、フランス、イタリア等**32カ国**、署名済み未締結国15カ国(カナダ等)（2011年11月現在）。なお、メンバー国で未署名国は4カ国(ロシア他)。

最新の締結国は、本年9月21日(2012年1月1日発効)の**スイス**。最近5年間では、2007年3カ国、2008年2カ国、2009年3カ国、2010年4カ国、2011年2カ国(11月現在)が批准、締結。なお、2010年には**トルコが署名のみを行った**。

我が国は、2001年署名後、**2004年4月国会の承認、2011年6月国内担保法の成立**、現在は締結のため、最高裁判所等で細部規則等を準備中。この作業には概ね1年を要すと聞く。

2　国連その他の国際機関の動きについて

（1）国連

国連では、主に、5年ごとに世界各地で開催される「**犯罪予防及び刑事司法についての会議**」（通称**コングレス**）で、参加国、国際機関、NGO及び個人の専門家等が集まり、犯罪防止・刑事司法全般にわたって、広い角度から議論を行い、勧告、提言等を行っている。

昨年4月、ブラジル・サルバドルにおいて、「**第12回国連犯罪防止・刑事司法会議**」が開催され、「グローバルな課題に向けた包括的戦略：変化する世界における犯罪防止・刑事司法制度とその発展」をテーマに議論され、「**サルバドル宣言**」の中にその成果が書き込まれた。

なお、**中国、ロシアは、これまでに、この条約**に反対する立場から、

「・**サイバー犯罪対策に関する条約は、国連において策定されるべきもの**である。

・本条約ではサイバーテロや新たな手口によるサイバー犯罪に対応できない。

・相互援助のため、自国にあるコンピュータから他国のコンピュータ･データにアクセスできること
などを認める本条約第32条bを受け入れることはできない。」
と主張している。
この他、中国、ロシアは、反対行動の一環として、政策レベルで次のような行動を取っている。

●2009年、上海協力機構加盟国間で「国際情報セキュリティ保障の政府間協力協定」に署名。

●2011年9月、国連事務総長へ「**情報セキュリティ国際行動規範**」を提出。
(同規範は、国家によるサイバー空間の主権管轄(国家によるサイバー空間での権利や自由の管理)、サイバー兵器・関連技術の規制、サイバー空間における資源の公平な配分の確保などを記述。)

●ロシアは2006年以降国連総会第一委員会に「国際安全保障分野における情報及び電気通信分野の進歩」決議案(**「サイバー決議案」**)を提出しているが、本年度決議案に新たに追加した文言が原因で、西側諸国が共同提案国入りしなかったという。

●その後、2011年10月、ロシアは「CONVENTION on INTERNATIONAL INFORMATION SECURITY(CONCEPT)」を、我が国を含めた各国に提示している。

（2）G8・サミット

サイバーセキュリティやサイバー犯罪について、年によって濃淡はあるが、**司法・内務大臣等による閣僚会議が中心になって**G8が強い関心や意見表明等を示している。

●**2008年**の**東京宣言**：かなり具体的にコミットした。

●**2009年**の**ローマ閣僚会議最終宣言**では、
①サイバー犯罪とサイバー・セキュリティを**議題として**取り上げ、
②**サイバー犯罪の危険性**は、技術進歩の速度と歩調を合わせ増大するとの認識を示し、
③ソーシャル・ネットワークや、暗号化サービス等情報システムに対する**新たかつ進歩した犯罪的攻撃が拡大しており**、法執行機関の能力の向上が必要だとし、
④この種の脅威への対処は、最も脆弱な社会階層、特に**若者と年配者を含むインターネット利用者の権利**を尊重しつつ、**プロバイダと法執行機関との協働**を改善することが不可欠、
⑤G8各国によるサイバー犯罪に関する**幅広い協働を奨励している**。

●**2011年ドーヴィルサミット**の**首脳宣言**中では、
①インターネット上の安全は、利害関係者が多く、犯罪目的で情報通信技術が利用されることを防止し、**(サイバー攻撃を)抑止し、処罰**するためには、各国政府、地域機関及び国際機関、民間セクター等の連携強化が必要、
②インターネットを通じた有害ソフトの拡散及びボットネットによる攻撃を含め、インフラ、ネットワーク及びサービスの公正性に対する攻撃には、特別な注意が必要、
③インターネットが、**平和・安全以外の目的、かつ、重要システムの公正性に悪影響を与え得る目的**で使用される可能性があることに懸念が示された。

（3）欧州評議会(Council of Europe)

欧州評議会は、1949年に創設され、47参加国家からなり、サイバー犯罪条約を支持する主要な組織である。現在も引き続き、**各国が有効なコンピュータ犯罪法を制定することを支援**しており、各種の機会に促進支持の行動を起こしている。

2010年4月28日、300以上の**法執行機関や産業界、他の専門家が**フランス・ストラスブールでサイバー犯罪カンファレンスを開催し、ネットワーク乱用問題やインターネット・ガバナンス組織と法執行機関との連携問題について議論した。今年も11月21日～23日まで開催した。なお、この条約は欧州評議会という一地域諸国が合意したものであり、この条約に参加するには、特別な要件を定めており、本年

11月23日、**オーストラリア司法大臣が**、条約成立10周年記念の特別会議で演説し、条約参加の意向を表明した。

（4）NATO

北大西洋条約機構(NATO)においては、最高意思決定機関である北大西洋理事会(NAC)がNATOのサイバー防衛に関する政策と作戦を統括している。2010年11月に公表された「**新戦略概念**」は、サイバー攻撃を予防・検知する能力、サイバー防衛能力及びサイバー攻撃被害から回復能力の強化を図り、全てのNATO機関を一元化されたサイバー防護の下に置くとした。2008年のエストニア事件以降、**サイバー防衛演習**を毎年実施している。

なお、NATOサイバーセンターが、2009年から学者、専門家に委託して、サイバー紛争に適用しうる国際法のマニュアルを検討中であり、2012年度末最終成果を発表する予定。

3　米国

米国は、2009年5月に発表した60日間の「**サイバー空間政策見直し**」に基づき**サイバーセキュリティ調整官**を**ホワイトハウス**に新設し、サイバーセキュリティ政策について関係省庁間の調整を行うこととした。

また、2011年5月には「**サイバー空間のための国際戦略**」を発表し、外交・防衛・開発援助の分野についてサイバー空間における**米国政府のビジョンを提示し、**優先的に取り組むべき**7つの政策分野**として、経済、**ネットワーク防護、法執行、軍事**、インターネット・ガバナンス、国際的な能力構築、インターネットの自由を挙げた。

そして、同年7月14日に発表された「**サイバー空間運用戦略**」は、米国によるサイバー空間の支配や軍事化に対する国際社会の懸念を意識して、刺激的な部分は非公開としたが、特に、（1）国防総省と軍のシステムに対する攻撃の大部分を妥当な自衛策によって防ぐこと、（2）国防総省・軍と相互依存関係にある外部のシステムの脆弱性を、運営者との情報共有によって改善していくことを強調している。

更に、国防総省のリン副長官は、重要なネットワークを攻撃するツールが存在することや攻撃により物理的損害が生じうること、主要システムのパフォーマンスに影響が及びうることなどに鑑み、サイバー攻撃への取り組みの戦略的転換を進めると説明し、新たな戦略の中核は、攻撃を阻止あるいは最小化することにあるとした。

具体的項目としては、（1）サイバー空間を陸海空同様の作戦領域と位置づける、（2）センサーシステムやウイルスなどの悪意あるコードの伝播や活動を阻止するシグネチャ技術、ソフトウェア等の活用により、アクティブサイバー防衛等の新たな作戦概念を導入する、（3）主要インフラ防衛等で国土安全保障省等他の政府機関や民間事業者等との連携を進める、（4）同盟諸国等との連携を図り、情報収集を進める、（5）ネットワークセキュリティを強化し、サイバー技術・人材の増強等技術的前提を変える、の5項目とを戦略の柱として示した。

体制的には、米国では、**国防省を除いた連邦政府**のネットワークや重要インフラのサイバー防護に関しては、**国土安全保障省**が所管しており、同省の**国家サイバーセキュリティ部**(NCSD)が戦略目標の設定や全体的な総合調整を行う。また、2009年に国土安全保障省に新設された**国家サイバーセキュリティ・通信統合センター**(NCCIC)は、政府のサイバーセキュリティ関連機関の業務を統合し、24時間態勢の警戒監視センターとしての役割を担っている。

なお、**国防省**の取組としては、2010年2月に公表された「**4年ごとの国防計画の見直し**」(QDR：Quadrennial Defense Review)は、**国際公共財**(グローバル・コモンズ)として陸、海、空、宇宙とともにサイバー空間を掲げ、国際公共財への**アクセスを保証**することが肝要だとし、更に、サイバー空間における効果的な作戦を、米軍の戦力を強化すべき6つの任務領域のうちの一つとしている。**組織面**では、

2009年6月に決定されたサイバー空間における作戦を統括する**サイバーコマンドが**2010年11月から本格運用を開始した。
2010年10月、**国土安全保障省と国防省は覚書**を締結し、国家全体のサイバーセキュリティ戦略の策定、能力開発のため、相互支援等により、両省の協力体制を拡大する人員、装備及び施設の提供についての枠組を取り決めた。

4　英国

（1）概要

英国では、2009年6月「**サイバーセキュリティ戦略**」が公表され、政府全体のサイバーセキュリティ戦略の立案・調整等を行う**サイバーセキュリティ部**(OCS)を**内閣府**の下に設置し、サイバー空間の監視等を行う**サイバーセキュリティ運用センター(CSOC)**を**政府通信本部(GCHQ)**の下に設置した。このOCS及びCSOCは、政府横断的な組織になっていたが、その後改編があり、OCSは情報保証部門と統合し**サイバーセキュリティ・情報保証部(OCSIA)**となった。

また、2010年10月に公表された「**国家安全保障戦略**」(NSS)及び「**戦略防衛・安全保障見直し**」(SDSR)は、サイバー攻撃を最も優先度が高いリスクの一つとして評価するとともに、国防省内のサイバー活動を一元化する**国防サイバー作戦グループ(DCOG)**の新設を決定している。

（2）2011年サイバー犯罪条約の締結

オバマ大統領と英国のデイビッド・キャメロン首相が、2011年5月会談を行い**サイバーセキュリティ**について一層緊密に取り組むことで同意したが、英国はこのタイミングでサイバー犯罪条約を批准した。

（3）新たな動き（ロンドン会議）

2011年11月1日～2日、英国のロンドンにおいて、サイバー空間に関するロンドン会議が開催された。この会議は、**ヘーグ英外相が主催**し、60カ国の政府機関他、国際機関、民間セクター、NGO代表など約700名が参加した。また、英国のキャメロン首相や、**インターネット中継**により**バイデン米副大統領**もスピーチを行った。

会議は、全体会議及び**5つのテーマ**からなる**分科会**等から構成され、インターネットの経済的・社会的恩恵を維持し、また、サイバー空間における犯罪的・安全保障上の脅威からいかに身を護るべきかという問題等について議論された。

(主な発言振り返り)

- **ヘーグ英外相**は、会議冒頭、サイバー空間の安定を図るにあたり、基本的人権、特に表現の自由が守られることが重要であり、検閲といった国家による過度な規制は不適切である。また、サイバー空間の発展、安定に向けた取組は、政府、企業、国際機関等が一体となって取り組む必要がある旨を述べた。
- **キャメロン英首相**は、①サイバー空間の発展があらゆる地域の人々に対して経済発展の機会を提供すること、②**サイバー犯罪への対応**が世界中の国々にとっての喫緊の課題であること、③サイバー脅威への安全保障上の対策が必要であることの3点が特に重要である旨発言した。
- **バイデン米副大統領**は、①サイバー空間における政府の排他的な権限行使は、サイバー空間の発展を停滞させるとともに各国との信頼関係を破壊する、②既存の国際法の原理・原則は、サイバー空間にも適用されるべき、③サイバー空間の安全の確保は各国政府のみの取組だけでは困難であり、**時間をかけてグローバルな基準や合意を形成**することが重要とした上で、**サイバー犯罪条約の促進と**サイバー空間での信頼醸成措置の重要性を述べた。

5　オーストラリア

（1）概要

同国では、これまでに数千件以上の攻撃があり、海外からの攻撃で議会のネットワークがダウンしたこともあった。

政府は、2009年11月に「**サイバーセキュリティ戦略**」を策定し、ハッキングや国家絡みのサイバー攻撃に対処する防衛戦略の更なる作成に取り組み、12年にはその詳細な計画が完成する見通しとなっている。

具体的には、司法長官が議長を務め、省庁間委員会である**サイバーセキュリティ政策調整**(CSPC)**委員会において**、危機管理や国際的な連携を含む政府全体のサイバーセキュリティ政策を調整・統括するほか、司法省にガブサートである**CERT Australiaを**新設し、民間事業者に対する脅威情報の提供や、事案対処の支援を行う。

（2）サイバー犯罪対策強化の改正法案

グローバル企業や政府等を狙ったサイバー攻撃が多発する中、オーストラリア政府は2011年6月22日、取締りを強化するための改正法案を公表した。

この法案が成立すれば、同国の警察や情報機関は通信会社に対し、通常ならば消去されるような情報の保存も強制でき、また、他国のサイバー犯罪取締機関との連携も強化され、自国の犯罪捜査に際し海外の情報にアクセスしやすくなる。

同国**法相は、この法案は**、国際的に唯一拘束力のある「サイバー犯罪条約」にオーストラリアが正式加盟するための**法的枠組み**となると述べ、2011年11月23日ストラスブーグで開催された同条約の10周年特別会合でキーノートスピーカーとして演説し、「新年のオーストラリア国会で承認をもらえれば、サイバー犯罪条約に加入する」と述べた。

6　韓国

韓国では、「韓国情報保護白書」等において、サイバーセキュリティに関する国家レベルの**一元的管理体制の必要性**が指摘されている。

国家サイバーセキュリティ政策等については、**国家情報院長**が統括・調整を行い、その下に、**国家サイバーセキュリティ戦略会議を**設置し、国レベルのサイバーセキュリティ体制の確立及び改善、関連政策及び機関間の役割調整、大統領の指示事項に関する措置や施策等の重要事項を審議している。

なお、2010年1月、国防情報本部の下にサイバー司令部が設けられ、サイバー空間における作戦の計画、実施、訓練及び研究開発を行ってきたが、2011年4月に、更に情報任務を付与され、**国防部直轄部隊に変更された**。

7　シンガポール

2011年11月、シンガポール政府は、多様化するサイバー犯罪に対応するため、国内を標的とするサイバー犯罪の早期発見と予防能力の向上を目指し、内務省の管轄下に新組織を設置し、政府が迅速かつ効率的に対処できる体制を整えると公表した。名称は「**国家サイバーセキュリティーセンター**」の予定で、3年以内に本格稼働をめざす。

なお、この新組織設置のほか、同国では**国際刑事警察機構（インターポール）**が2014年までに、一般犯罪対策の一環としてサイバー犯罪に対処する国際センターを設置する予定がある。