



日本原子力研究開発機構機関リポジトリ
Japan Atomic Energy Agency Institutional Repository

Title	核セキュリティ対策; サイバーセキュリティの側面から見て
Author(s)	福井 康人
Citation	CISTEC ジャーナル,(190),p.208-219
Text Version	出版社版
URL	https://jopss.jaea.go.jp/search/servlet/search?5070029
DOI	2021.1.25 現在なし
Right	安全保障貿易情報センター

核セキュリティ対策： サイバーセキュリティの側面から見て

日本原子力研究開発機構 福井 康人

1. はじめに

最近の代表的な脅威として2001年9月11日に起きた航空機による同時多発テロに見られるテロがあげられる。これには銃機乱射事件や大型自動車の無秩序な運転により短時間に大きな数の死傷者を生じる等様々な事案もある。特に日本では日本海側のみならず太平洋側の海岸にも原発が比較的集中して建設されていることもあり、昨今の不安定な朝鮮半島情勢や中東情勢等も相俟って、非国家主体の特殊工員のようなテロ攻撃の訓練を受けた者により、原発が襲われないかと危惧する声もある。もっとも原子力施設を巡る防護についてはその重要性が国際的

にも認識され、既に複数の国際条約が合意されているのみならず¹、国際原子力機関（IAEA）はこうした核セキュリティ分野²の国際約束を補足するために、核セキュリティ・シリーズの文書体系³が検討された上で公開されている。このように条約から重層的なソフト・ローの文書体系により、原子力施設に対する核セキュリティの在り方が詳細に至るまで規定されている。

また、2020年2月10日から14日までの期間、オーストリアのウィーンにおいて、国際原子力機関（IAEA）の主催により、「核セキュリティに関するIAEA国際会議（ICONS 2020）」が開催されており、その際には、若宮健嗣外務副大臣（当時）が日本政府を代表して、我が国の核セキュリティに関する方

¹ 例えば、核によるテロリズムの行為の防止に関する国際条約（略称：核テロ防止条約）（International Convention for the Suppression of Acts of Nuclear Terrorism）, 2245 UNTS 89, (enter into force 7 July 2007);

核物質の防護に関する条約（核物質防護条約）（Convention on the Physical Protection of Nuclear Material）, 1456 UNTS 246(entered into force 8 February 1987); 改正核物質防護条約（2005 Amendment to the 1979 Convention on the Physical Protection of Nuclear Materials）（adopted on 8 May 2016）があげられ、日本はいずれも締結している。

² IAEA Doc. IAEA INF/CIRC/225/Rev.5, June 2012, p.4, para.2.1.

核物質、原子力施設の物理的防護に関する核セキュリティ勧告（INF/CIRC/225/Rev.5, IAEA 核セキュリティ・シリーズ13番）によれば、その目的を核物質及びその他の放射性物質が関与する悪意のある行為から人、財産、社会及び環境を防護することにあるとした上で、以下の4点を挙げている。

- ① 不法移転に対して防護すること。
- ② 行方不明の核物質を発見、回収すること。
- ③ 妨害破壊行為に対して防護すること。
- ④ 妨害破壊行為の影響を緩和又は最小化すること

³ The IAEA's Nuclear Security Series はコンセンサスの得られたガイダンスをまとめたものであり、核セキュリティの基本的事項、勧告、実施ガイド、技術ガイダンスの4種類の文書からなり、核セキュリティの法体系の中では条約でないものの、ソフト・ローとして核セキュリティ関連法体系の重要な要素を形成している。

針を国際社会に説明すべく、演説を行った⁴。同演説では「核テロの脅威が依然として国際社会の安全保障に対する最大の挑戦の一つであり、原子力施設への攻撃をはじめとする潜在的な脅威が存在する。」とする。更に、「今世紀に入って核テロ対策を要する原子力施設も大幅に増え、(途中は省略) 技術の進化の結果、原子力施設等の物理的防護措置だけでは核テロ対策は十分でなくなり、今や内部脅威対策やサイバー攻撃対策など、多様な脅威を念頭に置いた取組が必要とされている。」との基本認識が示されている。

本稿テーマに関連する一般的な参考文献としては、『サイバー攻撃の国際法 (タリンマニュアル 2.0 の解説)』⁵ があげられ、これは我が国の核セキュリティ政策や本稿では省略されている武力紛争法も含めて戦時を想定したタリンマニュアル 1.0 のいわゆる平時版の抄訳である。また、最近スウェーデンの著名シンクタンク SIPRI が出した Cyber-incident Management: Identifying and Dealing with the Risk of Escalation⁶ が上げられるが、同政策ペーパーでは日本年金機構のデータベースがハッキングを受けた事例も含めて、9つの事例の分析も含めた考察がなされている。なお、特に核セキュリティの最新の動向をまとめた IAEA 報告書が 2020 年 IAEA 総会の際に「2020 年版核セキュリティ報告書」⁷ として作成されており、簡潔な記述であるもののサイバーセキュリティ対策も取り上げられている。

本稿では核セキュリティについて多様な側面がある実態にも考慮して、上述の副大臣のステートメントに述べられているサイバー問題に関連したものを中心に論じることとするが、まず、核セキュリティの関連の国際法を見るとの観点から、日本が締結している核セキュリティ関連条約及びそれを補完する IAEA 核セキュリティ文書について解説する。その上で、サイバー関連の重要な国際約束であるサイバー犯罪条約、更にはサイバー関連の国際会議や国連での動き等についても述べる。ちなみに、原子力施設に対するサイバー攻撃の中には、理論上武力紛争に相当するものも考えられなくもないが⁸、多くの場合はサイバー犯罪のカテゴリーに属するものであり、我が国の核セキュリティ政策も、警察当局の実力による排除を前提とした制度設計となっているので、その前提に基づき議論を進める。

2. サイバー攻撃の脅威

このような認識を踏まえ、本稿では特に原子力施設へのサイバー攻撃対策に焦点を当てて論じることとし、内部脅威対策についても関連する事項について触れる。事実、原子力発電所等を標的としたサイバー攻撃は増えており、サイバー問題を研究する国際政治学者の土屋大洋慶應大学教授が相次ぐ原発等へのサイバー攻撃として、いくつかの具体例の概要

⁴ 若宮外務副大臣の核セキュリティに関する国際会議出席 (結果)

若宮外務副大臣政府代表演説 at https://www.mofa.go.jp/mofaj/dns/inec/page3_003061.html (as of 12 October 2020)

⁵ 本書は Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, February 2017, Cambridge University press, を基にした抄訳版であり、最初のタリンマニュアルが戦時を想定しているに対して、同マニュアルは平時のサイバー攻撃を想定した解説用日本語抄訳である。

⁶ Cyber-incident Management: Identifying and Dealing with the Risk of Escalation, SIPRI, September 2020, pp.1-50

⁷ IAEA Doc. GOV/2020/31-GC (64)/6*, “Nuclear Security Report 2020,” 27 July 2020, pp.1-35.

⁸ ジュネーブ諸条約第一追加議定書第 56 条 1 項は「危険な力を内蔵する工作物及び施設、すなわち、ダム、堤防及び原子力発電所は、これらの物が軍事目標である場合であっても、これらを攻撃することが危険な力の放出を引き起こし、その結果住民たる住民の間に重大な損失をもたらすときは、攻撃の対象としてはならない。これらの工作物又は施設の場所又は近傍に位置する他の軍事目標は、当該他の軍事目標に対する攻撃がこれらの工作物又は施設からの危険な力の放出を引き起こし、その結果住民たる住民の間に重大な損失をもたらす場合には、攻撃の対象としてはならない。」と規定し、原子力発電所への攻撃は明示的に禁止されている。この規定の趣旨に鑑み、原子力発電所以外の原子力施設であっても危険な力を内蔵する施設への攻撃は禁止されると解される。

また、万が一、警察力で対処できない事態に至った場合は、通常の日国内で想定されている核セキュリティの対処手順とは異なる事態対処法等の別の国内法体系のレジームに依拠して対応することとなり、日本政府内での主務官庁も原子力規制庁から内閣官房等別の指揮命令システムに移行することになるものと思われる。

を引用している⁹。そこでは2011年3月の東日本大震災では福島第一原子力発電所では地震で外部電源が失われたために、起動した内部電源を津波が襲って喪失して制御システムだけでなく、すべてのシステムがシャットダウンした。その教訓として、原子力発電所は予め定められた手順に従った慎重な運用だけでなく、設計からあらゆる事態を想定する必要がある。このような事例にみられるように、自然災害が引き金となった重大事故が発生したが、意図的に攻撃される重要インフラストラクチャーへのサイバー攻撃やサイバーインシデントも、実は随分前から発生している点を著者は指摘している。

具体的にみると、同書には明確に原子力施設を標的とした攻撃の事例4件があげられている。まず、1992年2月にバルト3国の一つであるリトアニアのイグナリナ原子力発電所で技術者が意図的にコンピューター・ウィルス¹⁰を制御システムに感染させるという事件が起きた。また、2003年1月には、米国オハイオ州のデービス・ベッセ原子力発電所において、SQLスラマーというワームによって安全監視が5時間機能しなくなった。2007年9月、シリアで建設中の核施設が見つかったが、この核施設は間もなくイスラエルによって空爆されてしまう。事前にシリアのレーダー網に対してサイバー攻撃が行われており、シリアは飛来するイスラエル戦闘機を見つけられなかった。サイバー攻撃と物理的な攻撃を組み合わせると非常に効果的であることを示した。最後の事例は2014年12月には、韓国水力原子力発電(株)(KHNP)に対する情報抜き取りのサイバー攻撃が行われたとされている。

筆者も東日本大震災当時には外務省の5階にいて、耐震強化工事が行われているものの、庁舎が激しく揺れて生きた心地がしなかった。その際に福島

第一原子力発電所では津波により内部の非常用電源も喪失した。結果として、全ての電源を喪失し、原子炉の冷却水循環が出来なくなり、炉心が溶解する一方で水素爆発により隣接する施設を含めて建屋が損壊して、放射性物質が大気中に漏れる事態になったことは記憶に新しい。このことから、津波でなくとも、何らかの形で電源を喪失すると類似の緊急事態が生じる可能性があることが明らかになった。また、2010年7月にはイランのナタンズのウラン濃縮施設では、マルウェアがクロズドな遠心分離システムに侵入し、遠心分離機を物理的に破壊するに至った事件も発生した¹¹。

こうしたことから、自然災害やテロが脅威となって不測の事態を招きかねないことが広く認識されるようになった。マルウェアによる制御コンピューターの動作異常や内部データが詐取されることが起きかねないとして、核セキュリティの観点からも原子力施設のサイバーセキュリティの確保が喫緊の課題となっている。特にこうした原子力関連施設へのサイバー攻撃により、施設が損壊して放射性物質が漏れるようなことが起きれば大変なことになることは火を見るよりも明らかであり、万が一サイバー攻撃の標的にされた場合は即座に且つ適切に対処する必要がある。こうしたサイバー攻撃の特徴は、瞬時には発生する上に、インターネットを経由して遠隔で攻撃が実施されることもある。ナタンズウラン濃縮施設ではUSBメモリー等可搬型デバイスまたは情報システムから侵入(Windowsネットワークのサービスの脆弱性を利用した可能性が指摘されている¹²)したとされているが、詳細は明らかにされていない。

また、このようなサイバー攻撃は、proxyサーバーや別のサーバー等を使った攻撃にさらされることも

⁹『暴露の世紀 - 国家を揺るがすサイバーテロ』土屋大洋、角川新書、195頁から197頁。なお、それ以外にも以下のNTIの作成した資料には、複数の事例があげられている。

Alexandra Van Dine, Michael Assante and Page Stoutland, Ph.D., OUTPACING CYBER THREAT: PRIORITIES FOR CYBERSECURITY AT NUCLEAR FACILITIES, NTL2016, pp.5-32.

¹⁰JIS X0008「情報処理用語—セキュリティ」at <https://cybersecurity-jp.com/security-measures/17886> (as of 16 October 2020)

コンピューター・ウィルスは、「自分自身の複写、又は自分自身を変更した複写を他のプログラムに組み込むことによって繁殖し、感染したプログラムを起動すると実行されるプログラム。」と定義されており、ウィルスは単体では存在しないが自己増殖するもの、ワームは単体でも存在するものの自己増殖する特徴があり、トロイの木馬型のなりすまし型を合わせて、マルウェアと称している。

¹¹村瀬一郎「制御システムセキュリティの重要性と現状：第2回原子力分野における制御システムセキュリティ」原子力学会学会誌 Vol.56-7,2014, 18頁 - 21頁

¹²「前掲論文」19頁。

あるが、上記の Stuxnet 事案のように内部の制御システムにアクセス権のある者が意図的にマルウェアとは知らずにシステムのメンテナンスの際に持ち込まれることがある。当然のことながら、その時点では破壊行為につながりかねない挙動はしないので、発見が困難であることは言うまでもない。このように、遠隔地からのサイバー攻撃、外見上は無害であり且つ制御システムに必要なソフトに仕込まれて、ある時点からマルウェアとして活動するものでもあるので、発見も容易でない場合があり、更に言えば犯行行為者の特定や犯人の帰属の確定が困難な場合も少なくない。

3. 核セキュリティ関連条約の概要と関連する IAEA の取組

(1) 核セキュリティ関連条約

まず、核セキュリティ関連条約としては冒頭にも言及した核テロ防止条約と既に改正済みの核物質防護条約が挙げられるが、本節では3条約を中心に核セキュリティ分野の国際約束の解説を行った後に、IAEAの作成した核セキュリティ文書の紹介を行う。先ず、核によるテロリズムの行為の防止に関する国際条約（International Convention for the Suppression of Acts of Nuclear Terrorism、略称：核テロ防止条約）については、当初はロシアが提出した国際テロリズム廃絶措置に関する国連総会決議（A/RES/51/210）に基づいて、1997年2月から国連総会第6委員会の下に国際テロ撲滅アドホック委員会が条約交渉機関として設立されて交渉が開始された¹³。この条約も、核兵器を巡る国連における南北対立といった国際政治の影響を免れることが出来ず、例えば条約第4条2項には「この条約は、いかなる意味においても、国による核兵器の使用またはその威嚇の合法性の問題を除外するものではない。」とする文言が注釈的に入れられている。これは、非同盟諸国が核兵器の使用が核テロリズムであると主張して議論が紛糾したため、このような文言を挿入することにより、この非同盟諸国の懸念は解消されて、

最終的に条約が作成された。

また、他方で核物質の防護に関する条約（Convention on the Physical Protection of Nuclear Material、略称：核物質防護条約）については、1974年の第29回国連総会において当時のキッシンジャー米 국무長官が国際輸送時の核物質に対する防護措置協定の必要性について演説したことについて端を発している。この条約は国連ではなく、専門性が高いことからIAEAにおいて、核物質防護に関する勧告の検討が開始された。特にそこでは核物質の国際輸送時の防護や核物質が関係する国際間の犯罪の取り扱いに関する国際協力が重要課題となった¹⁴。その結果、1979年10月に開催された政府間会合において同条約が採択され、1980年3月に開放された。同条約も全文及び23条の条文並びに2つの附属書からなっている。この条約も多くの条約と同様に第1条の定義と第2条の適用範囲に続き、第3条では国際輸送中の核物質の防護義務、第4条は核物質の輸入及び通過時の防護が規定されている。

更に、第5条は核物質防護及び回収のための締約国間の協力、第6条は情報の秘密の保護の必要性につき規定している。それ以外では第6条の情報の秘密性の保護、第7条の犯罪行為の処罰規定が特筆されるが、それ以外にも通常のテロ防止条約にあるような一連の刑事訴追関連手続、締約国会議といった意思決定機関や紛争解決条項がおかれている。また、附属書については、附属書Iが「附属書IIに区分する核物質の国際輸送において適用される防護の水準」、附属書IIが「核物資の区分表」をまとめており、同条約の規制対象が明確化されて、附属表を含めて改正は条約全本文体並びに改正会議を経ることとされている。

その後核テロ等の脅威に対する認識の高まり、この条約に加えて、防護措置の対象及び犯罪とすべき行為の拡大が行われたのが、核物質防護条約の改正であり、防護措置の拡大については「国際輸送中の核物質」に加えて「国内の核物質及び原子力施設」に改正するとともに、条約名も「核物質及び原子力施設の防護に関する条約」に改正された。更に、犯罪とすべき行為の拡大については「核物質の窃取」

¹³ 福井康人『軍縮辞典』日本軍縮学会編、2015年、信山社、97頁-98頁。

¹⁴ 宮本直樹『前掲書』日本軍縮学会編、2015年、信山社、110頁-111頁。

や「法律に基づく権限なしに行う核物質の使用等」から、「法律に基づく権限なしに行う核物質の移動（第三国間の移動を含む）」及び「原子力施設に対する不法な行為等」に拡大され、2014年6月に発効し、我が国は2016年5月に締結した。

なお、このプロセスは1999年11月にIAEAが招集した非公式専門家会合により検討が開始され、紆余曲折を経て2005年7月に招集された外交会議により改正案が採択された¹⁵、この核テロ防止条約及び核物質防護条約及び同条約改正の合計3条約が核セキュリティ分野の主要な法的拘束力を有する国際約束であるが、いずれにせよ核セキュリティの実施の企画立案はそれぞれの締約国が責任をもって実施することとなり、この方針はこうした条約のみならず、後述するソフト・ローを形成するIAEA核セキュリティ文書等でもこの方針は踏襲されている。

(2) IAEA 核セキュリティ関連文書

IAEAにおいては、米国同時多発テロ以降、4年毎に「核セキュリティ計画」を策定し、その中で「核セキュリティ・シリーズ文書」と呼ばれる一連の文書が発行されてきた。核セキュリティ・シリーズ文書は、基本文書、勧告文書、実施指針及び技術手引の順で階層的な体系として分類されている¹⁶。これらの文書は法的拘束力がない上に、上位規範ともいえる上述の国際条約と同様に具体的な国内実施措置はIAEA加盟国が国内実施については各国が主体的に決定することが出来、これは国により現行の核セキュリティ措置の実施レベルが異なる実態や施設の形態等が統一されていない状況下で実施するには適している。ちなみに、日本の場合は福島第一原子力発電所での事故を踏まえ、安全対策として津波対策の防護壁の設置等日本独自の措置が取られている。

これらの核セキュリティ文書の詳細は実際の文書を参照して頂くこととして¹⁷、代表的な核物質及び

原子力施設の物理的防護のコアになる概念について述べる。先ず筆者が感じたのは他の類似分野でも目にする事項があげられており、分野が異なっても意外に共通する面がある。先ず、事業者の責任が強調されており、防護措置には事業者が積極的に取り組むべき原則が強調されている。この点は事業者が実際に施設を建設して運用し、そこで勤務する職員を採用して雇用するのは各事業者であることを踏まえると、当然の帰結であると思われる。また、リスクベースの物理的防護のみならず、対応すべき脅威の拡張として内部脅威、遠隔攻撃及びサイバー攻撃等が挙げられている¹⁸。こうした論点の提示も昨今のサイバー攻撃事案を考えると、極めて自然な問題提起と思われる。

では、これまでに述べた関連国際条約の国内法担保について述べる。まず、核テロ防止条約は主に放射線を発散させて人の生命等に危険を生じさせる行為等の処罰に関する法律により国内担保が行われている¹⁹。もっとも同法附則第3条は、その後の国際立法の動向を踏まえ、「この法律の施行の日以後に日本国について効力を生ずる条約並びに核物質の防護に関する条約及びテロリストによる爆弾使用の防止に関する国際条約により日本国外において犯したときであっても罰すべきものとされる罪に限り適用する。」とし、核物質防護条約のみならず、爆テロ防止条約の国内担保法としても機能している。なお、原子力関係の基本的な法律である、核原料物質、核燃料物質及び原子炉の規制に関する法律（いわゆる原子炉等規制法）及び放射性同位元素等の規制に関する法律と相まって実施されることが法第1条の目的に明記してあり、こうした法律も当然のことながら関連する。

また、核セキュリティ・シリーズは条約でないものの条約を補完する形で作成されていることから事実上、上記の法律で担保されているのみならず、関

¹⁵ 宮本直樹『前掲書』日本軍縮学会編、2015年、信山社、111頁。

¹⁶ 寺林雄介『立法と調査』「核物質防護条約改正の経緯と主な内容」351号、2014年、参議院事務局、5頁。

¹⁷ Nuclear Security Series, at <https://www.iaea.org/resources/nuclear-security-series> (as of 8 October 2020)

例えば、2011年1月に公表された勧告文書は「Nuclear Security Recommendations on Radio Active Material and Associated Facility」を含めて上記もURLに公表されている。

¹⁸ 『電力中央研究所報告』「核セキュリティに関連する国際情勢の動向分析-INCFIRC/225/Rev.5への改定を中心に」調査報告Y10018、2011年、9頁。

¹⁹ 放射線を発散させて人の生命等に危険を生じさせる行為等の処罰に関する法律（平成19年法律第38号）、平成29年4月14日公布（平成29年法律第15号）改正、令和元年9月1日施行。

連する規則においても記載されている。一例をあげると、2018年5月にIAEAが公表した核施設での機器のコンピューター・セキュリティと制御システムについての核セキュリティ・シリーズ No.33-T には、様々な措置について記載されているが、例えば内部脅威については同文書では特出しして記載していないものの、複数個所に分散して書かれている。これが日本の場合は同文書を踏まえて、例えば、「実用発電用原子炉の設置、運転等に関する規則」第91条第2項18には「情報セキュリティ計画」作成の必要性が述べられている²⁰。

最後に、核セキュリティに関連する国際協力枠組みについて述べると、先ず、「核テロリズムに対抗するためのグローバル・イニシアティブ」があげられる。これは2006年7月のG8サンクトペテルブルク・サミットに際し、米露両国の大統領は、核テロリズムの脅威に国際的に対抗していくことを目的として、「核テロリズムに対抗するためのグローバル・イニシアティブ (Global Initiative to Combat Nuclear Terrorism: GICNT)」を提唱したことに端を発しており、IAEAとは異なった同志国による協力枠組みとなっている。更に、政治的ハイレベルのものとして、2009年4月、オバマ米大統領がプラハ（チェコ）において演説を行い、核テロは地球規模の安全保障に対する最も緊急かつ最大の脅威とした上で、核セキュリティ・サミットを提唱して核セキュリティの重要性がハイレベルでも認識されるに至っている²¹。

4. サイバー犯罪条約の概要と関連する動き

近年は原子力施設に限らず、中央官庁等様々な場所でのホームページのサーバーへの侵入や書き換えから始まり、金融システムへの侵入等枚挙にいとまがなく、例えば、大量の暗号資産であるビット・コインが消滅して大きな社会問題となったことも記憶に新しい。このため、日本政府も2014年にサイバーセキュリティ基本法を定めて、内閣官房長官を本部長とするサイバーセキュリティ戦略本部が設置されて、内閣官房直轄の重要事項として関係する官庁を構成員とする政策決定を行っており、2018年7月にはサイバーセキュリティ戦略²²が閣議決定されるなど今日においても日本政府の重要政策の一つである。その一方で、サイバー技術はAIと同様に日進月歩の技術進歩をしており、NISC（内閣サイバーセキュリティ・センター）が様々な防御情報等により注意喚起を行っている。

(1) サイバー犯罪条約

サイバー問題は多岐にわたるものの、前節で扱った核セキュリティの文脈でも重要視されており、核セキュリティに関する ICONS 2020 において当時の若宮外務副大臣が行った政府代表演説においても、「原子力施設等に対するサイバーセキュリティ対策の一層の強化」の必要性を訴え、具体的な脅威として、内部脅威対策及びサイバー攻撃対策について言及されている。こうした考えは会議で採択された閣

²⁰ 実用発電所原子炉の設置、運転等に関する規則第91条2項18は「発電用原子炉施設及び特定核燃料物質の防護のために必要な設備又は装置の操作に係る情報システムは、電気通信回線を通じて妨害行為又は破壊行為を受けることがないように、電気通信回線を通じた当該情報システムに対する外部からのアクセスを遮断すること。」と規定し、同19は「前号の情報システムに対する妨害行為又は破壊行為が行われるおそれがある場合又は行われた場合において迅速かつ確実に対応できるように適切な計画（第96条第1項において「情報システムセキュリティ計画」という。）を作成すること。」を規定している。これは規則であるものの、規制庁と事業者の監督官庁からの指導の形で関連する作業が行われるので法律と同等の強制力を有しており、同規則からの逸脱も事実上許容されない。

²¹ 核セキュリティ・サミットは、これまで合計4回開催されている。

(1) 2010年4月：ワシントン核セキュリティ・サミット開催。成果文書としてコミュニケ及び作業計画を採択。

(2) 2012年3月：ソウル核セキュリティ・サミット開催。成果文書としてソウル・コミュニケを採択。

(3) 2014年3月24日及び25日：ハーグ（核セキュリティ・サミット開催。成果文書としてハーグ・コミュニケを採択。

(4) 2016年3月31日及び4月1日：ワシントンで総括会合が開催され、コミュニケを採択したほか、輸送セキュリティに関する共同声明を日本がリード国として取りまとめを行った。

²² 2018年7月27日付け閣議決定「サイバーセキュリティ戦略」

at www.kantei.go.jp/jp/singi/it2/dai61/siryou5.pdf (as of 12 October 2020)

僚宣言にも反映されており²³、IAEA 加盟国からも支持を得ている。もっとも、このようなサイバー攻撃のほとんどは、警察による実力の行使で対処し得る場合がほとんどであり、日本が締結している条約では、サイバー犯罪に関する防止条約（略称：サイバー犯罪条約）を活用することが可能である。

サイバー犯罪は、原子力施設に対する攻撃の場合も該当するが、犯罪行為の結果が国境を越えて広範囲な影響を及ぼし得るという特質を与えていることから、例えば、同時に国外から別のサーバー等を複数経由して複数の施設を攻撃することも可能である。また、コンピューター・ウィルスの中には、標的に到達すると直ちに作動するものもあるが、そのまま潜伏して一定期間後に作動開始するものもあり、作動しなければ発見が困難なものも普通のウィルスでなく、OS等に常駐してコンピューターは一見普通に作動して効果的な防御が困難なものもある。このため、その防止及び抑止のために国際的に協調して有効な手段を講じる必要がある。こうした背景からまずは先進国中心の欧州において、そのために法的拘束力のある国際条約の作成が必要であるとの認識が、最初に欧州評議会において共有された。

このため、欧州評議会の下で、サイバー犯罪を取り扱う専門家会合が設置されて、1997年以降この交渉フォーラムにおいて交渉が進められ、最終的に2001年9月に行われた欧州評議会閣僚委員会代理会合においてこの条約の案文に合意することが出来た。同年11月8日に開催された欧州委員会閣僚委員会会合において正式に採択されて、その後ハンガリーのブダペストで署名式が行われた。なお、同条約第37条は非加盟国の加入についても規定しており、「欧州評議会閣僚委員会は、この条約の締約国と協議してすべての締約国の同意を得た後に、この条約の作成に参加しなかった欧州評議会の非加盟国に対してこの条約に加入するよう招請することができる。」と規定されていることから、日本もこのような加入招聘手続きに基づき、2012年7月3日に受諾書を

提出して当事国となっている。

サイバー犯罪条約は、原子力施設を対象としたサイバー攻撃対応にも当然のことながら適用可能であり、この条約が禁止する行為の範囲に入ることがなされると締約国は国内法に基づき禁止する必要がある。即ち、一般的にはサイバー犯罪から社会を保護することを目的として、コンピューター・システムに対する違法なアクセス等一定の行為の犯罪化、コンピューター・データの迅速な保全等に係る刑事手続の整備、犯罪人引渡等につき規定するものである。問題となるのはこのような国際条約があっても、現実にはサイバー攻撃者や不法行為の責任の帰属の特定が容易ではないことであり、例えば複数国のサーバーを経由して攻撃が実施された場合に、途中の国の中に同条約の締約国でない場合は国際協力の鎖が切れてしまうことになる。

そのような問題が存在するのは事実であるも、いずれにせよ締約国間では国際協力の規定が機能し、締約国でない国とも協力を謳っている同条約は有益なサイバー問題解決のためのツールとして機能しており、前文、48条及び末文からなっている。サイバー犯罪条約は、先ず第1条の定義で、「コンピューター・システム」、「コンピューター・データ」、「サービス・プロバイダー」及び「通信記録」の基本的概念が定義されている。そのうえで違法なアクセス及び違法な傍受及び第3条について規定しており、第2条はコンピューター・システムに対するアクセス、第3条はコンピューター・データの非公開送信に対する技術的手段による傍受が権限なしに故意に行われることを犯罪化することを求めている。

更に、データの妨害及びシステムの妨害については、第4条がコンピューター・データの破損、削除、劣化、改ざん又は隠蔽が権限なしに故意に行われることについて、更に第5条がコンピューター・データの入力、送信、破損、削除、劣化改ざん又は隠蔽によりコンピューター・システムの機能に対する重大な妨害が権限なしに故意に行われることの犯罪化

²³ MINISTERIAL DECLARATION, International Conference on Nuclear Security: Sustaining and Strengthening Efforts, 10-14 February 2020, pp.1-2. at <https://www.iaea.org/sites/default/files/20/02/cn-278-ministerial-declaration.pdf> (as of 12 October 2020)

同会議終了時に採択された閣僚宣言第10段落には、「我々は、原子力関連施設におけるコンピューター・セキュリティに対する及びサイバー攻撃からの脅威並びに核物質及び放射性物質の使用、貯蔵及び輸送を含む原子力関連施設に関連する活動に対する脅威を認識するとともに、加盟国に対し、機微な情報及びコンピューター・システムの保護を強化するよう求め、また、IAEAに対し、この関連で、国際協力を促進し、要請に基づいて加盟国を支援するよう奨励する。」とされている。

を各締約国に求めている。更にはそういった行為のための装置の濫用（第6条）、コンピューターに関する偽造及び詐欺（第7条及び第8条）等についても併せて規定されているが、いずれの規定も国内法により犯罪される場合は、いずれも「故意に」行われる条件が課されており、規定によっては「権限なしに」行われることが要件に課されている。これはうっかりとした操作でも同じようなことがコンピューターの場合は起こりうる現状を考慮したものと思われる。

もっとも、こうした行為の犯罪化に当たっては未遂罪及びほう助罪又は教唆についても定めている。即ち、第2条から第10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犯罪の実行をほう助し又は教唆すること、並びに第3条から第5条まで、第7条及び第8条並びに第9条の一部の規定に従って定められる犯罪であって故意に行われるものの未遂罪の創設についても規定されているものの、締約国は別途留保することが認められている、これは事情を斟酌せざるを得ないような場合や逆に積極的に取り締まる必要があるような、特に本稿で扱う原子力施設で取り扱うような事案の場合は犯罪の抑止効果を十分に確保する必要があるため、こうした様々な要因を勘案することが出来るようにされているものと思われる、締約国の裁量の範囲が確保されている。

更に、第16条の規定する再発防止や犯罪捜査に極めて重要なのが蔵置されたコンピューター・データの迅速な保全である。これは他の電磁的記録でも同じであるが、電子データは簡単に記憶装置のデータ構造等を熟知していれば消去は比較的簡単であり、不正アクセスの痕跡も消去することが可能である。このため、自国の権限ある当局がコンピューター・システムによって蔵置された特定のコンピューター・データ（通信記録を含む）の迅速な保全を命令すること又はこれに類する方法によって迅速な保全を確保するために、立法措置をとることが出来るとしている。これは他の蔵置されたコンピューター・データの捜索及び押収（第19条）と共に、捜査や司法上の要請のみならず、攻撃を受けた施設で再発防止策を検討したりするためのみならず原状回復に重要な働きをする規定である。

ではこうしたサイバー犯罪条約であるが、日本の

国内法的にはどのような形で行われているのだろうか。これも昨今はパソコン等でも無線LANが使われることが多くなっていることや有線LANによりコンピューター間の通信が行われることから、データの通り道となる回線に対する規制をかける必要があることから、先ず、電波法及び有線電気通信法の改正を行う必要が出てくる他、情報処理の高度化等に対処するための刑法等の一部を改正する法律が改正された。しかしながら重要なのは、核セキュリティ分野のサイバー攻撃に限らずサイバー犯罪条約の国内担保法のうち、不正アクセス行為の禁止等に関する法律（平成11年法律第128号）である。この中でも、要となるのは不正アクセス行為の禁止を規定する法第3条の「何人も、不正アクセス行為をしてはならない。」と定められていることである。

(2) サイバー犯罪条約の国内実施と核セキュリティ

特に核セキュリティとの結節点としては、同法附則平成11年12月22日法律第160号等に記載されているものの多くが、更に下部規範に記載されているため、法律レベルではそれほど明確に出てこないものの、核セキュリティのところでも述べた実用発電用原子炉の設置、運転等に関する規則といった文書にわずかに出ているのみであるが、この規定に従い、施設ごとに詳細な情報セキュリティ計画が作成されて、本件の主務官庁たる原子力規制委員会の認可を受けた上で運用されている。当然のことながら、このような文書が外部に出ると、確実に当該施設のセキュリティ対策に支障をきたしかねないので、規則に従い、施設の設計情報と共に厳重に管理されており、秘密保全措置の対象になっている。

また、過去に起きた事例から、内部からの施設設計情報が漏れたことにより、制御系システムにアクセスし得たものと思われるもの、本人が知らないうちにメモリースティック等の記憶媒体を通じてコンピューター・ウィルスが持ち込まれた可能性がある。このため、無線・有線を問わず回線を経由してのみならず、ウィルスに感染した記憶媒体を持ち込むことが施設の規則で禁止された上で、そのようなことを行う可能性のある人物を予め排除する必要がある、これが内部脅威対策の重要な点である。もっともこれは内部脅威の一例であり、どのような行為が内部脅威になるかは、例えば、施設の防護情報を外

部に漏洩することも更なる攻撃を可能にすることから十分脅威になるし、施設内で破壊行為を行うことも該当するなど多様な形態で脅威となることを認識する必要がある。

もっとも、当該施設の管理者でなくても、例えば、警察や公安調査庁関係者が職務として破壊活動を行う可能性のある自然人や法人を調査するにしても、人権上の配慮が必要とされることは言うまでもない。即ち、法令上は関係者から報告徴収権限がある場合であっても、令状の請求が必要等法の適正手続が取られた上で、設置法や内部規則に従って調査を行う必要があり、こうした配慮が必要になってくる。その上で、関係者の人定事項等を確実に把握し、施設で勤務する人がその施設に危険をもたらさないようにする必要がある。そのためには、本人のアクセス時に不要なものを施設入域時に不要なものを持ち込ませない等と合わせて措置を講じる必要がある。

(3) サイバー関連国際会議

また、視点を変えてサイバー関連国際会議と関連しうる国連の対応についても敷衍すると、日本の外務省が公表しているだけでもかなり多くの会合がこれまでも行われている²⁴。まず首脳レベルで開催されるものについては、サイバー空間に関する国際会議は既に5回ハイレベルで開催されている。これは2011年11月にロンドンで開催された会議を端緒として、第2回目会合が2012年にブダペストで開催され、第3回会合が2013年にソウルで開催されて最初のラウンドを終えた。更に、第4回会合が2015年にハーグで開催され、直近では2017年にニューデリーで開催されている。いずれの開催地もサイバー問題には熱心な国である。

それ以外にも国連総会第一委員会に提出された決議に基づいて、情報セキュリティに関する政府専門家会合(GGE)が近年では6回開催されており、日本も第3会期以降は参加国に選出されている。2019年には第1回オープンエンド作業部会が開催された

が、国連を舞台とした条約交渉にはつながっていないのが現状である。広く知られているように、国連憲章第2条4項には国際関係における武力の行使が禁止されているが、伝統的な解釈は経済戦争を含まず、有形力の行使を前提とした議論が伝統的に展開されてきた²⁵。しかしながら、有形力の行使に比するようなサイバー事案が発生し始めたため、この憲章2条4項による武力の行使に含まれるのかといった問題のみならず、国連憲章第51条の規定する集団的自衛権のトリガーとなりうるのかといった論点が議論されるようになってきた。

更に、一般論としてサイバー問題に国際人道法や国家責任法が適用されるのかといった問題も議論されるようになり、タリンマニュアルのような国際人道法研究者を中心に議論も開始された。もっとも、これまでに開催されたGGEでもこうした問題も取り上げられるようになってきた結果として、こうした問題に対しても肯定的且つ積極的にとらえようとする国もあるものの、例えばキューバのような国は最終段階で議論をブロックして、GGEはコンセンサス報告書を採択することが出来なかった²⁶。このように、米国等西側諸国がサイバー問題を推進しようとする中、P5の中でもロシアや中国は足を引っ張ろうとして、議論は国連のような加盟国数が増えると途端に有志国会合のようにはいなくなる多数国間外交の現実がある。特に核セキュリティといった切り口に限定せず、一般論としてサイバー問題を扱おうとすると、表現の自由との関連や児童ポルノ対策といった様々な要素も入ってくるため、議論での合意が更に難しくなる傾向がある。

このため、サイバー問題の特定の関心事項にテーマを限定して、同士国又は二国間協議により議論を深化させるとともに、攻撃を受けた際の捜査協力を含めて当局同士で協力関係を構築する方が、効率の良い取組を可能にするという実情も大きく働いていると思われる。確かにサイバー空間に関する会議では多様な側面が扱われて、サイバー問題への取組に

²⁴ 国際組織犯罪に対する国際社会と日本の取組：サイバー犯罪
at <https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html> (as of 12 October 2020)

²⁵ Bruno Simma et al., "The Charter of the United Nations: A Commentary (Oxford Commentaries on International Law)," Oxford University Press, 2013, p.209.

²⁶ Michael Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms," 30 June 2017, at <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/> (as of 10 October 2020)

ついでに政治的気運を盛り上げる効果はあるのは事実である。他方で、国連といった多数国間外交の場に持ち込むと、どの分野でもそのような傾向があるが先進国が強力に推進しようとする、そうした動きを懸念する開発途上国もいるために、条約等に合意することが必ずしも容易ではないとの傾向がある。このため条約化は欧州評議会といった比較的共通項の多い国同士で合意された条約をベースに、その普遍化に協力しつつサイバー犯罪や、核セキュリティ対策といった特定分野に特化したフォーラム、即ち IAEA の様な専門家の集うフォーラムで原子力施設に対するサイバー攻撃対策の検討を進める方が効果的であるものと思われる。

5. 結びにかえて

筆者は本稿を執筆する際に勤務先の関係者から差し障りのない範囲で聞き取り調査を行った他、勤務先の採用時の研修でヴァーチャル・リアリティを活用した核セキュリティの訓練施設を見学する機会を得たが、事柄の性質上、筆者がそれを詳らかにすることは、「見えざる敵」を利することになりかねないので、核物質防護等の観点から許容されない。特に本稿で扱う施設の保全は、特に核セキュリティ及びサイバーセキュリティという2重のセキュリティが要求される重い案件であり、しかも重要インフラである原子力施設であるがゆえに、万が一攻撃が成功すると、最悪の場合、放射性物質が大気中に放出され、あたかも「汚い爆弾 (Dirty Bomb)」による攻撃が行われたように多くの生命が危険に晒されかねないのみならず、原発であれば大規模な停電というような社会的影響の大きい大規模事案が発生しかねない点に留意する必要がある。

このため、筆者も過去の職業でなじみのあった在外公館警備等とは異なった意味で非常にデリケートであり、防御に失敗すると重大な結果をもたらすことになる。他方で、どのような防御態勢がとられうるのかは、警備会社等は商用目的から自社の扱うセ

キュリティ関連機器の一般向けのカatalogを公開していることが多いので、その傾向をある程度知ることが可能である。このため、核関連施設でこのような問題を担当する者は、こうした情報はある程度公知の事実となっており、最悪の場合は施設に脅威をもたらしかねない潜在的テロリストはこのような公開情報を入手した上で攻撃してくる可能性があることを十分に留意した上で、対策を講じる必要がある。

例えばその一つの例は、日本の電機メーカー研究者が執筆した「原子力計装制御システムのサイバーセキュリティ対策の現状と展望」²⁷があげられる。同論考には発電所におけるサイバーセキュリティ確保のため、中央計装や計装制御に用いられるデジタル設備に対するセキュリティ対策を講じるとともに、万が一のサイバー攻撃に備え、セキュリティ状態を監視する SOC (Security Operation Center) やセキュリティ事故時に復旧対応を行う CSIRT (Cyber Security Incident Response Team) などを配置し、セキュリティ統合管理システム、セキュリティ事故手順書を整備することで迅速な対応を実現するための計装制御システムにおけるサイバーセキュリティ対策の全体構成を図で示している²⁷。

これによると具体的な構成要素として、①記憶媒体チェック装置 (発電所に持ち込む記憶媒体のセキュリティを確保)、②セキュリティチェック装置 (ウイルス対策、ホワイトリスト等によりシステム内のセキュリティを確保)、③データダイオード装置 (物理的な一方方向のデータ通信を実現して重要システムへの侵入を防止)、④セキュリティ状態の監視 (発電所内のデジタルシステムへの侵入の検出)、⑤セキュリティ事故対応措置 (SOC、CSIRT 等の組織の実現によってサイバー攻撃時の事故復旧対策の実現)、⑥迅速なセキュリティ事故後復旧対策 (セキュリティ事故手順書や訓練設備等によってサイバー攻撃時のセキュリティ能力の向上) の6要素からなるシステム設計を想定している。

そこで中心となるのは現場ではいわゆる SOC や CSIRT であり、専門的知識を有し機器の操作も可能な要員のみならず、状況を把握して対処すべき措置

²⁷ 稲葉隆太、町田慎弥「原子力計装制御システムのサイバーセキュリティ対策の現状と展望」『三菱電機技報』Vol.90, No11, 2016, pp.23-25. なお、こうした施設の実際のサイバー攻撃対策も 2019 年に公表された『原子力規制委員会情報セキュリティポリシー』に準拠してシステムが構築され、運用されている。

を迅速に判断する分析員の存在が不可欠であり、問題となる事象が発生してから事故対処を行いつつ、システムのダメージを最小化し、正常な状況まで復旧させるオペレーションが必要となって来るが、それを実施するのはシステムのみならず、「人」が中心である。事業本部といった遠隔地に所在する指揮所と連絡を取り、時には専用の診断ソフトウェアを活用しつつ、起きてしまった事故の状況を分析し、システムを復旧させるのに活躍を期待されるのは普段からよく訓練された担当要員である。ここで考慮すべき問題は機材については調達して適切に設置すれば機能するが、「人」の即時養成は不可能なので、人事管理部門と調整しつつ、更には内部脅威対策としての人選のスクリーニングも勘案しつつ、中長期的観点から必要な人材を養成した上で関連部署に配置していく必要があることである。

また、サイバー攻撃の際に守るべきものも、施設内で異なっている点についても留意する必要がある。

例えば、通常の原子力施設では情報システムそのものと計装制御システムの双方が通常の原子力システムにおいて混在していることが少なくない。しかしながら、情報システムの守るべきは個人情報、資産情報、経営情報といった情報資産であり、その資産はサーバー等の通常の機器に置かれていることが多いため、通常の汎用セキュリティ機器により情報防護が可能である。他方で、計装機器システムに置かれる情報は保存計測データや操作履歴であり、情報防護よりも防護すべきは単なる取得されたデータもさることながら、実際に機能している機器も含めて防護の対象とする必要がある²⁸。

このように両者は同レベルの情報防護では不十分であるものの、基幹業務サーバーを含む情報システムも計装機器システムも、例えば、通常の執務室の隅に設置するのではなく、専用のサーバールームに設置されるべきであり、双方とも一般職員が勝手に操作出来る状況にあるのが好ましくないことはある意味当たり前である。しかしながら、職場によっては意外に守られていないことも多いし、極論すれば花瓶が割れて水浸しになるような場所においてはならないのは、至極当然であろう。筆者が長年見てき

た職場等ではつまらないことではあるものの、意外にこうした基本的なことも守られず、そのような意識ではサーバー運用をしている職員により高度なサイバー対策を講じても徒労に終わりがねない。このため、広い意味で核セキュリティ及び情報セキュリティの双方につき、関係するセキュリティ要員のみならず、施設で勤務する一般職員についても、核セキュリティ及び情報セキュリティの双方についての研修等セキュリティ・カルチャーの醸成の機会を設けることも重要である。

以上、より具体的な核セキュリティとサイバー問題について、事例を踏まえながら述べたが、筆者がこの問題に興味を持ち、以前から中長期的な課題として重要であると考えている問題を本稿の結びとして述べたい。

まずサイバー攻撃の特徴は一瞬にしてやられることがあるので予め特殊な対応が必要ということである。もっとも、サイバー攻撃には時限爆弾型もある他、武力攻撃に相当して事態対処法等の対象になりうる可能性も否定出来ないが、多くはその前の段階でサイバー犯罪レベルの対応が中心となるので、まずは警察力による排除を前提に考える必要があり、筆者は特に以下の3点を強調したい。

第1点は、サイバー攻撃は瞬時にして攻撃を受けることが多いので、普段からサイバー攻撃の踏み台となるような弱点を防ぐことが重要である。具体的に考えられるのは、侵入経路となりうるポートを放置したりするなどといったセキュリティ・ホールは残さないことである。これは識者には釈迦に説法であるかもしれないものの、新たな機器の設置をした際に、保守業者が自分たちの作業用に `guest account` を設置したまま削除せずに放置したままのサーバーを実際に見たことがあるが、こうしたセキュリティ上の弱点があると、コマンドが使用可能なユーザーであればネット上から簡単に侵入することが可能である。

第2点目は、本稿で取り上げたサイバー攻撃は原子力施設という特殊な施設を標的した攻撃であり、原子力規制庁、警察、契約警備会社といった特定の組織で技術的諸元は把握されているものの、サイバー技術は日進月歩の技術であり、遠方の国から国

²⁸ Ibid. 「前掲論文」 p.25.

家レベルで攻撃をしたことが疑われる事例もある。
このため、常に新たな事案研究を行い、防御能力の維持向上を図る必要がある。このような実情にかんがみ、内閣官房、総務省、経済産業省、防衛省等のサイバー関連部門の国内の知見を有する機関の専門家との交流により新たな情報を得て、サイバー攻撃の可能性を小さくするための方策を定期的に部内で検討することも必要である。

第3点目として、特に警察等法執行機関が果たすべき役割の中で、サイバー攻撃実行者の特定は処罰、再発の防止の観点から重要であり、本稿で扱う事例は原子力施設が絡んでいるために被害が甚大になる可能性も否定できず、そのためには国際協力は不可欠であると思われる。特に原子力関連施設防護の関連では、核セキュリティの強化とともにサイバー攻撃対策を同時に強化することは重要である。この観点から、サイバー犯罪条約の普遍化は核テロ防止条約の普遍化と合わせた両輪として推進の必要があると言える。

特に、来年の2021年には改正核物質防護条約のレビュー会合が予定されており、こうした機会を捉えて日本等の主要国が主導して、例えば、将来のレビュー会合に向けた国際的にもアクションプランが検討の上、策定されるなど、関連条約の運用状況が向上する機会を創設することが強く望まれる²⁹。我が国は東日本大震災の際に国難ともいえる試練を乗り越えることを余儀なくされたが、一步一步確実に復興の道を歩んでおり、こうした機会にそうした苦難を乗り越えた我が国の姿を世界に示すことが出来ることを望んでやまない。

²⁹ IAEA Doc. GC (64)/RES/10, September 2020, pp.1-9. para. 5.

例えば、2020年IAEA総会にてコンセンサスで採択された核セキュリティ決議には、本文パラ5に「ICONS2020の閣僚宣言を考慮し2022～2025年のIAEA核セキュリティ計画を策定するよう各加盟国に呼びかけ」の文言が新たに加わったことを考慮した上で作業を進めるのが効率的と思料される。