論　説

サイバー・フィジカル・セキュリティの維持に関する政策的議論及び罰則の現況

西　貝　吉　晃

第１章　本研究(1)の背景と目的

サイバーフィジカルシステム(CPS)(2)という言葉が聞かれるようになった。サイバー空間におけるデータ処理とフィジカル空間の事象とがセンサ群(フィジカル⇒サイバー)、出力系(サイバー⇒フィジカル)により高度に融合したIoTシステムのことである(3)。スマートホーム、スマー

(1)　本研究には複数分野の知見を総合して利用している部分が多く、読みにくい部分もあるかもしれない。そこで、本研究のダイジェスト的な議論を西貝吉晃「サイバー・フィジカル・システムに対するサイバー攻撃と刑法的対応―コネクティッドカーの事例を参考にして」櫻庭信之＝北條孝佳＝行川雄一郎編著『法律実務のためのデジタル・フォレンジックとサイバーセキュリティ』(商事法務、2021年刊行予定)にてまとめてもいるので適宜参照されたい。

(2)　この概念は技術的にも異なる様々なシステムを捕捉するが、ここでは、物理世界の情報をサイバー空間で処理し、物理世界に返すという物理世界とサイバー空間との間のインタラクションを担うシステムだと理解しておく。小さな組み込みシステムから、自動車、航空機、さらには国レベルのインフラまでもがCPSの一種である(山田直史＝高島洋典＝木村康則「超スマート社会(Society5.0)実現に向けてCPS/IoTとその後」情報管理60巻５号325頁、326頁(2017))。

トファクトリー(4)といった言葉もCPSの一種である。水道や電力等の社会インフラもそれがネットワークを介して物理的に制御されれば(スマート化されれば)CPSである(5)。医療に目を転じればCPSとしての心臓のペースメーカーも考えられる。

こうしたCPSのセキュリティの維持・向上をどう図っていくかが現在、大きな社会的課題となっている(6)。ハッキングによってより直接的に物理的な障害を惹起できてしまう点でCPSは高度なリスクに直面している(7)。既に様々なシステムの脆弱性が問題視されている。例えば、電気手術器に対して不正なコードを実行可能にしてしまう脆弱性が発見されたり(8)、航空機のエンタメシステムへの侵入を起点とした航空機の制

(3)　Society5.0における新たなガバナンスモデル研究会「GOVERNANCE INNOVATION ver. 2 2.4アルゴリズムの判断によるフィジカル空間への作用アジャイル・ガバナンスのデザインと実装に向けて」報告書案(執筆時現在、意見公募手続中)2.1以下参照。入力の多様さについて指摘するものの、それ以降の過程についてはフィジカル面をそれほど重視しないものにトレンドマイクロ「IoTセキュリティガイドライン―デバイス ライフサイクルの概要―」がある。同ガイドラインの2020年５月更新版の２頁では、IoTの世界における処理過程には　(1)センサーによるデータの収集　(2)プロセッサによるデータの処理　(3)ネットワーク／ゲートウェイを介したデータの接続　(4)有益情報を得るためのデータ分析に基づいた意思決定　(5)スマートアプリケーションの生産性を向上させるための情報活用　(6)セグメンテーションに恩恵をもたらす新たな様々なインテリジェンスサービスにおける情報活用の６つのステップがあるとする。センサによる入力系の拡張もIoTの重要な特徴であるが、むしろ、本稿では、出力系におけるフィジカル面の多様性に着目して研究を行いたい。

(4)　スマートファクトリーのセキュリティについて佐々木弘志「スマート工場における組織およびシステムの総合的なセキュリティ対策」計装61巻６号59頁(2018)、上野広行「つながる工場・組込機器セキュリティ」計測技術47巻９号14頁(2019)、山田ほか・前掲注(2)326頁(2017)、トレンドマイクロ・前掲注(3)３頁。

(5)　山田ほか・前掲注(2)326頁。

(6)　奥家敏和「「Society5.0」時代の産業サイバーセキュリティ」計測技術47巻９号１頁(2019)。

御システムの乗っ取りや自動運転車に対するハッキングによる遠隔制御の可能性が指摘されたりしている[9]。さらに、実際に原子力発電所のコンピュータにマルウェアが混入していた事例[10]、天然ガス圧縮施設がランサムウェアを使った攻撃を受け２日間操業停止に追い込まれた事例（図１参照）、水道における塩素制御装置等へのサイバー攻撃により水道施設のポンプが一時停止した事例（図２参照）[11]等が報告されている[12]。

上記の事例から観察できるとおり、重要インフラに対する攻撃は、従前はフィジカルの側面からなされる必要があったが（建造物侵入の後に制御システムを破壊する等）、それが現在ではリモートで可能である[13]。今やサイバー空間の安全は現実空間の安全と密接に関係しているといえ[14]、重要社会基盤事業者[15]により管理されている重要インフラに対す

⑺ James Davis, “Cybersecurity for Manufacturers: Securing the Digitized and Connected Factory”, 6（2017）、岩野和生＝高島洋典「サイバーフィジカルシステムとIoT（モノのインターネット）」情報管理57巻11号826頁（2015）。

⑻ 経済産業省商務情報政策局サイバーセキュリティ課「令和２年３月２日付『第２層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性」６頁。

⑼ 経済産業省商務情報政策局サイバーセキュリティ課「令和元年11月27日付『第２層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性」５頁。

⑽ BT-Drs. 19/1716, 1.

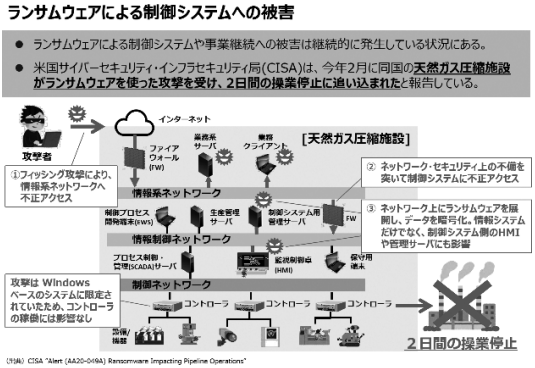
⑾ 以上の２つの事例について経済産業省商務情報政策局サイバーセキュリティ課「令和２年８月６日付『第２層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性」８、９頁。

⑿ さらにSociety5. 0における新たなガバナンスモデル研究会・前掲注⑶５頁以下。

⒀ サイバー・フィジカル空間のポリシーについての調査結果としてAnna Leppanen, Sari Kajantie & Timo Kiravuo, Policing the Cyber-Physical Space, 89 Police J. 290（2016）.

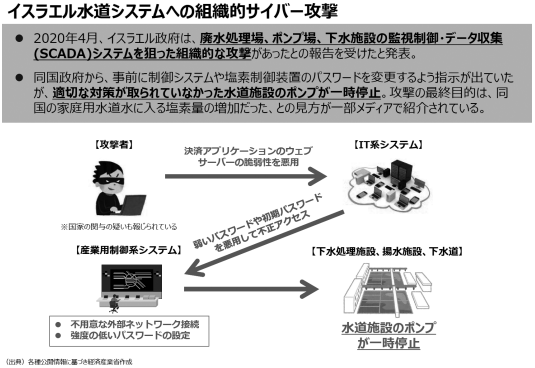
⒁ 神足祐太郎「サイバーセキュリティ政策の現状」調査と情報1078号１頁（2020）。

図１　天然ガス圧縮施設の被害事例



（出典）CISA "Alert (AA20-049A) Ransomware Impacting Pipeline Operations"

図２　水道システムの被害事例



（出典）各種公開情報に基づき経済産業省作成

るサイバー攻撃への対処については国家的施策が進んでいる。

全てのCPSが重要インフラであるわけではないが、重要インフラは保護の必要性の高いものとして議論の俎上に真っ先に挙がるものだといってよい。NISC（内閣サイバーセキュリティセンター）が発表した「重要イ

⑮　サイバーセキュリティ基本法３条１項内の定義によれば、国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者である。重要インフラの管理主体だと考えてよいだろう（神足・前掲注⑭５－６頁）。

ンフラの情報セキュリティ対策に係る第４次行動計画」においては、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット（クレジットカード決済システム）、石油を、重要インフラ分野として特定している[16]。保護すべき重要なインフラが十分に挙げられているといえよう。第４次行動計画別紙２[17]ではシステム障害が起きたときの報告に係る（各事業者を名宛人とする）法令、ガイドライン等も紹介されている。もっとも、立法論も含め、故意（場合によっては過失）による重要インフラに関連するシステム障害の惹起については、人命に対する危険が発生する可能性も大いにあるから、刑法上も強力な保護が要請される[18]。

こうした状況に鑑み、本研究では、CPSのセキュリティ維持・向上のために刑法がどのように寄与すべきか、ということを考えていく。CPSの明確な定義は難しく、同概念は何でも吸収し得る便利な言葉だと評される[19]。法的議論においてCPSそれ自体を漠然と使うことは推奨されない[20]から、ここでは、CPSの安全性を侵害する場合、つまりサイバー・フィジカル・セキュリティが侵害される場合を、「サイバー攻撃によってコンピュータによって制御されている物理的なシステムの物理的な挙動が変更され得る状態が作られること」を意味するものとして議論を進めたい。CPSの保護を考える上でも、情報セキュリティと同じく、発生し得るリスクを考える必要がある。もっとも、モノ自体及びモノが置かれた環境のデータを取得したソフトウェアがフィジカルな世界におけるモノのアクチュエート[21]を可能にすることを踏まえると考慮すべき範囲

---

⑯　第４次行動計画50頁別紙１。

⑰　第４次行動計画51頁以下。

⑱　既に夏井高人「サイバー犯罪の研究（五）」法律論叢86巻２・３合併号85頁、107頁以下（2013）。

⑲　中島震「CPS：そのビジョンとテクノロジー」研究技術計画32巻３号235頁（2017）。

⑳　ビジョンとしてのCPSは抽象的哲学的に過ぎるともいえ（中島・前掲注⑲244頁–245頁）、研究をするにあたって、一定の限定をかけることは各分野において求められ得る。

が広がるので、どのように議論の軸を構成するかがまずは問題となる。

以上を前提に、本研究では、国内の議論状況を整理することを目指す。すなわち、第２章においてサイバー・フィジカル・セキュリティの維持に関する政策的議論を、第３章及び第４章において、これに関する罰則の現況を紹介して、今後の研究課題を探る。

第２章　CPSのセキュリティに対する考え方

本章ではCPSのセキュリティに対する考え方をいくつか紹介する。前提として、既に情報化社会や高度情報通信社会の到来に伴い、サイバーセキュリティ及びその前身ともいえる情報セキュリティに関する議論の蓄積がある。情報セキュリティの議論においては、データを保存している媒体やシステム（情報システム）の保護が検討対象になることはあるが、情報の保護を最終目標に据えた議論が展開されていた。そこで保護対象となるのはCIA（機密性、完全性、可用性）であった。しかし、CPSのセキュリティを考えるということは、物理プロセスへの影響も考察することを意味しており、必ずしもCIAの保護のみでは足りない。既にITリスク学という分野が提唱されており、例えば重要インフラにITシステムが使われていることに起因して、いわゆるCIA（機密性・完全性・可用性）を超えた当該ITシステムの安全性の保護・維持の重要性が謳われている。さらに、2016年８月に公表された内閣サイバーセキュリティセンター（NISC）「安全なIoTシステムのためのセキュリティに関する一般的枠組」２頁において、IoTシステムのリスクが他のIoTシステムに波及する可能性があることに鑑み、上記のCIAに加えて「安全性」の保護が謳われている。

以上の背景事情を踏まえ、より具体的にサイバー・フィジカル・セキュリティの保護に向けた取組みを紹介・分析したい。

⑵1　福岡真之介編著『IoT・AIの法律と戦略〔第２版〕』12頁（商事法務、 2019）、山田ほか・前掲注⑵326頁。

第１節　経済産業省の取組み

第１款　サイバー・フィジカル・セキュリティ対策フレームワーク

第１項　内容の紹介

まず、経済産業省によるサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を紹介する[22]。CPSFは、あらゆるモノがネットワークでつながることを想定している「Society5.0」の実現に向けて、付加価値を創造する活動すべてがサイバー攻撃の対象に晒される可能性があると認識する[23]。その上で、考察のレイヤーを

①サイバー空間

②フィジカル空間とサイバー空間のつながり

③企業間のつながり

に分けて、セキュリティ対策のために必要な事柄の洗い出しを行う（CPSF13頁、図３参照）。各層でのセキュリティ対策要件が充たされることが確認でき（信頼の創出）、それを照会できるようにすることで（信頼の証明）、信頼のチェーンが構築され、サイバー空間とフィジカル空間が融合する社会における新たな価値創造を支援できるとする（CPSF21頁以下）。

②のレイヤーはデータ処理⇔物理的挙動の「転写」機能の保護が必要だという意図に基づいている。すなわち、②においてはセキュリティ上の脅威が機器の誤動作等の安全上の問題につながる可能性があるので、例えば、セキュリティ侵害の原因となり得る箇所や機器を特定する作業を行う[24]。

さらに、セキュリティ維持の考察対象として、ソシキ、ヒト、モ

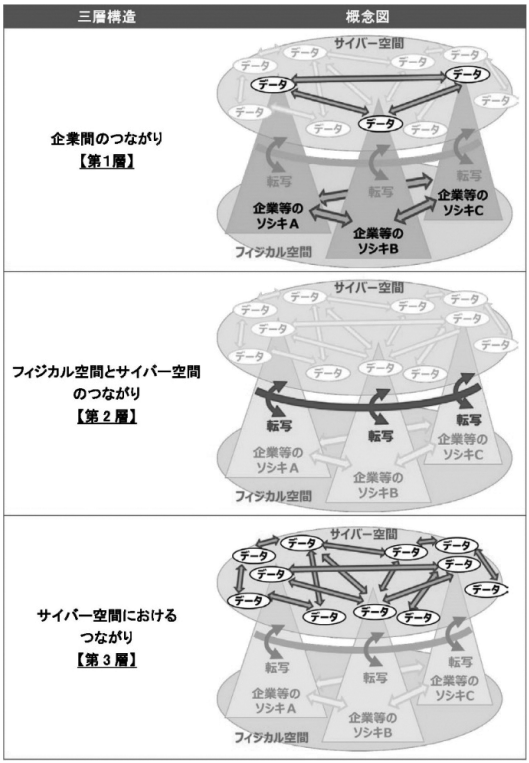
---

[22] サイバー・フィジカル・セキュリティ対策フレームワーク1.0（2019）（https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html）。CPSFから、IoT-SSFに至るまでの包括的な紹介として奥家敏和「サイバー・フィジカル・セキュリティ・フレームワークを活用したサプライチェーン・セキュリティの確保」情報処理62巻３号e7頁（2021）参照。

[23] 奥家・前掲注(6)３頁。

[24] 奥家敏和「「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」の策定と今後の取り組み」計装62巻８号９頁、11−12頁（2019）。

図３　３つのレイヤーで理解されるサイバー・フィジカル・セキュリティ



ノ[25]、データ、プロシージャ、システム[26]の６つの最小単位を設けて検討している（CPSF17頁以下）。CPSのセキュリティを考える際には、企業のような組織が重要な主体となってくる。

第２項　検討

以上を前提に、３つのレイヤーに分けた議論に着目して考察を行ってみたい。CPSへの攻撃により②における処理が妨害された場合には、法

⑵5　ハードウェア、ソフトウェア及びそれらの部品というように、ソフトウェアを含むとされていることに注意。

⑵6　目的を実現するためにモノで構成される仕組み・インフラ。

的には、そのことを理由に処罰すべき場合があるかもしれない。もっとも、①、②への攻撃がなされないように、③の企業に対し、セキュリティマネジメントを政策的ないし法的に要請すべき場合もあるかもしれない。その意味では①、②、③の３つに考察のレイヤーを分けることには合理性があり得る。

しかし、フィジカル空間への影響は、火災や交通事故等の事象として認識できて、②とも区別し得るから、②と③の間に③として「フィジカル空間への影響」を追加し、さらに現状で組織となっている事柄について、スマートホーム等においては、対個人の侵害も問題になるから、①、②、定義し直した③に加え、組織に代わる視点として④として「社会的影響」のレイヤーを作るのが、より一般的な議論を展開する上ではよいように思われる。以上をまとめると次のようになる。

①サイバー空間の保護
②サイバーとフィジカルの間の「転写」機能の保護
③フィジカル空間の保護
④社会的影響

もっとも、④の例をあらかじめ示し、法的思考との関係で関連性がある程度に具体化して類型化する必要があろう。

第２款　IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）

次に、第１款で紹介したCPSFの議論を土台に置きつつ、さらに、統一的な評価を試みるものとして、規制との関係を強く打ち出したものではないが（IoT-SSF４頁）、IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）が2020年に公開された[27]。

IoT-SSFでは、IoT（Internet of Things）をサイバー空間とフィジカル空間をつなぐ機器・システムの代表例として捉える（IoT-SSF４頁）。IoT機

[27] 既に総務省において、サイバーセキュリティタスクフォース「IoT・5Gセキュリティ総合対策 プログレスレポート2020」が公開されていた。そこでは、重要インフラ等の社会的に影響を及ぼすリスクを伴った使用をしているIoT機器（重要IoT機器）について、公開する必要のない情報が公開されているなど、攻撃を受けやすい脆弱な状態にあるものを検出すること等の重要性が指摘されている（同レポート資料８）。

器・システム[28]にも、簡易な情報サービスの分野に使用されるIoTから、工場や社会インフラシステム等の安全に関わる分野で使用されるIoTまでのものが含まれ、インシデントが起きた際の社会的影響の程度や求められるセキュリティレベルにも大きな多様性があり得る。もっとも各業界でのケースバイケースでの判断を放任すると、社会的コストの増大を招き得るから、一定の統一的な判断手法が求められる(IoT-SSF３頁−４頁)。こうした状況に鑑み、IoT-SSFは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するための「基本的共通基盤」を提供し、IoTという新たな仕組みを社会として効果的に受容できるようにすることを目的として作成された(IoT-SSF４頁)。

IoT-SSFは、インシデントによって様々なリスク(利益侵害)が発生し得ると指摘する。例えば、人命に関わるようなケースもあれば、プライバシーに関わるケース、資産の毀損に関わるケース、生活環境に関わるケースもある(IoT-SSF５頁)。もっとも、多様に過ぎるリスクを類型化して整理することは問題を過度に難しくするという考慮から、様々な人命／身体、プライバシー／名誉、資産、生活環境、経済活動への影響、風評等の影響を受ける様々な事象を、発生したインシデントの影響の回復困難性の度合いと発生したインシデントの経済的影響の度合い(金銭的価値への換算、 社会的な混乱の程度)の２つの軸から抽象的に分析して、それぞれのIoT機器・システムが、その用途に応じて、どのようなリスクを孕んでいるかを分析している(図４参照)。右上にカテゴライズされるものほどインシデント発生時の影響が大きい傾向があるため、より重厚な対策が必要であり、左下にカテゴライズされるものほど、軽微な対策で十分な可能性があると整理し得る(IoT-SSF８頁)。

こうしたマッピングを経ることで、第３軸としてのセキュリティ・

---

[28] IoT-SSFではIoT機器とIoTシステムを分けていない。考察対象が機器であっても、システムであっても、IoTの有するポテンシャルから付加価値が提供される点では同じであるからあえて区別しなかったのである(IoT-SSF２頁)。

図４　リスクに応じたIoT機器・システムのマッピング方法

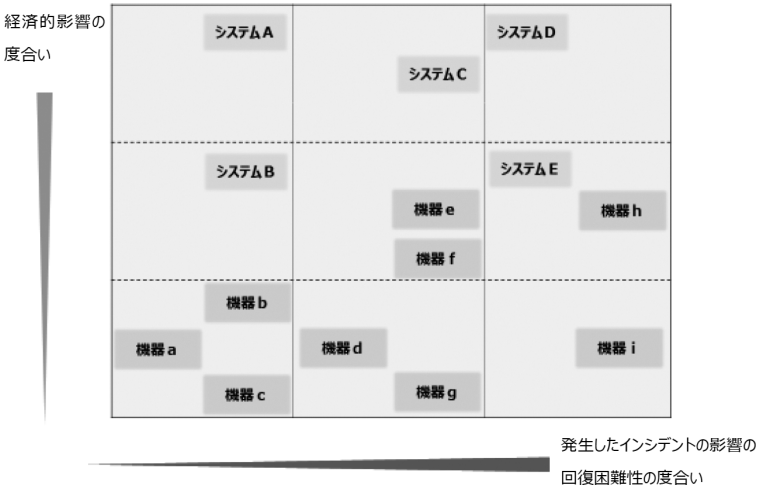


図５　マッピングされたリスクの程度に基づいた社会的な仕組みの要求

セーフティ要求として、社会的な措置のあり方を可視化できる（図５参照、IoT-SSF 10頁）。第３軸において、具体的なセキュリティ対策のあり方を検討する際の視点として、IoT機器・システムの運用前及び運用中における確認要求、IoT機器・システムの管理者の能力の確認要求、その他の社会的な仕組みの要求が挙げられている（IoT-SSF 11頁）。

IoT-SSFの議論は、刑事的・行政的な規制を念頭に置いたものではない。インシデントの発生を前提とした法的措置というよりは、インシデントの発生を未然に防止したり、発生したとしてもその被害を最小限に食い止めたりするための社会的な仕組みのあり方を問うものである。刑法では重要な議論となってくる被害法益の類型化の観点がショートカットされているのも、例えば誰かを処罰することを念頭に置いたものではないことを理由として正当化することができよう。

もっとも、そのようなIoT-SSF６頁が、リスクについて次のように述べる点は注目に値する。「『リスク』については、インシデントによる影響の度合いと、インシデントの起こりやすさ[29]を用いて捉えることがあるが、本フレームワークでは、フィジカル・サイバー間をつなぐ機器・システムの多様性を踏まえたカテゴライズが容易に行えるように、算出が比較的難しい起こりやすさは考慮せず、インシデントが発生した場合の影響の度合いからカテゴライズを行うアプローチを採っている」。この議論方法により、インシデント発生の蓋然性の問題をひとまず外に置き、発生の蓋然性は低いが、どうしても発生を抑止しなければならない重大な利益侵害を伴うインシデントを「重要なリスク」として認識することが可能になる。それは、（経済合理的な見地から一定のリスクを受容し得る場合を認める）情報セキュリティからのアプローチよりはむしろ、刑事立法学のアプローチに近いものがある[30]。

ただし、それでも、刑法的な議論を行う際には、侵害される法益の類型化作業に踏み込まなければならない[31]。そこでさらにヒントを得るために、第２節で制御システムのセキュリティに関する議論を参照する。

---

[29]　例えばIPA「制御システムのセキュリティリスク分析ガイド 第２版」20頁（2020）を参照。

第２節　制御システムのセキュリティ

第１款　サイバーセキュリティの延長線にあるCPSのセキュリティ

制御システムに対するリスクマネジメントについて既に一定の議論がある（IEC62443[32]）。そこでは、物理的リスクのアセスメントの結果とHSE（Health（健康）、Safety（安全）and Environment（環境））上のリスクのアセスメントの結果とサイバーセキュリティリスクのアセスメントの結果の統合が図られる必要がある[33]、と指摘される。制御システムにおいては物理プロセスが保護対象となる[34]。データ保護の優先順位に関しても、制御システムに関しては、要保護性の順番がAIC（可用性、完全性、機密性）に変わり[35]、保護対象にさらに財務（Business）およびHSEも追加される[36]。

⑶⓪　例えば、後述する新幹線の運行の安全を刑法的に保護しようとする文脈で、新幹線の特殊性について、「万一事故が発生した場合におけるその被害がきわめて大きいと予想される」と述べられていた（井上五郎「東海道新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法解説」曹時16巻11号46頁、47頁（1964）、伊藤栄樹「東海道新幹線における列車連行の安全を妨げる行為の処罰に関する特例法について」警察学論集18巻５号10頁、13頁（1964））。そこでは事故が発生する蓋然性が極めて小さくても、それが発生した場合における被害の大きさに基づいて刑事立法の必要性が検討されている。

⑶①　刑法の関心事は、究極的には法益侵害の質、量といえるからである（神山敏雄「コンピュータ妨害の刑事法上の考察」警察研究58巻５号28頁、32頁（1987））。

⑶②　制御システムを保護するための方策について定めた一連の規格。2018年後半から欧米日の企業で導入が進められているようである（村上正志「IoT/第４次産業革命時代 サイバー攻撃から「制御システム」をどう守るか」計測技術47巻９号６頁、９頁（2019））。

⑶③　4. 2. 3. 11.

⑶④　熊谷洋子＝松原佑生子＝内山宏樹＝鍛忠司＝藤田淳也＝中野利彦「制御システム向け事業レベルでのリスク分析手法の提案」情報処理学会論文誌60巻９号1518頁、1523頁（2019）。

⑶⑤　既にIPA「制御システムセキュリティとITサービス継続に関する調査」21頁（2009）。

もっとも、CPSのセキュリティ（制御システムのセキュリティ）と情報セキュリティとは類似する点も多い。むしろCPSセキュリティは要件加重されたものだともいえる。IPA（独立行政法人情報処理推進機構）[37]は、制御システムのセキュリティに関するIEC62443-2-1の要件と情報セキュリティ（ISO/IEC27001）の要件の大半が共通していることを指摘している。

セキュリティ上の留意事項自体をある程度共有しているがゆえに、サイバーセキュリティ上の保護を行うことでフィジカルシステムに対する保護も一定程度図ることができそうである。

第２款　被害の類型化と刑法への応用可能性

ここで、熊谷らは、悪影響の定義をＨ＆Ｓ（人的安全性）、Ｅ（環境的安全性）、Ｂ（事業継続性、公衆の信頼、法的制裁）の観点から表１のように分類している[38]。引用の際に、影響レベルの程度（軽微と甚大の例が各セル内に記載される形式）を横軸にして少し修正した。

法学の立場からすると、他の事実的な被害と法律の評価が並べられていることについて疑問はある。まず、犯罪に対しては社会的非難をもって臨むべきであって、軽重はあれども罪を犯したことを社会的に軽く見

表１　制御システムのセキュリティの議論における被害の類型化

観点	リスクの種類	影響レベルが軽微	影響レベルが甚大
Ｈ＆Ｓ	人的安全性	疾病の発生	死亡事故の発生
Ｅ	環境的安全性	地域行政への報告が必要な汚染	広範囲、長期間の汚染
Ｂ	事業継続性	限定範囲での事業停止	広範囲での事業停止
	公衆の信頼	顧客信頼の喪失	ブランドイメージの喪失
	法的制裁	軽い刑事犯罪	重い刑事犯罪

---

(36)　熊谷ほか・前掲注(34)1523頁。

(37)　IPA「制御システムにおけるセキュリティマネジメントシステムの構築に向けて～IEC62443-2-1の活用のアプローチ～」16頁（2012）。

(38)　熊谷ほか・前掲注(34)1522–1523頁。

るべきではないことを踏まえると、影響レベルが軽微の項目に犯罪を入れることは相当でない。また、そもそも、ある事実を法的に評価してその重大性を考えるという法学的思考からすると、(思考の無限ループに陥るから、)Bの中に法的制裁があるべきではない。H＆Sにおける死亡事故の発生が故意又は過失で行われたとしても、殺人罪や業務上過失致死罪に問われ得る。さらに、(よりよい法規制を考える場合に、)既に存在する法的制裁を検証するだけでは足りず、法的制裁以外の部分の各セルの事実が法的制裁に値するか否かを考えていくことが重要な事柄となる。

一方で、この表からは、リスクマネジメントの観点からの影響レベルの評価方法をくみ取ることもできる。これは法的分析の観点からも一定の参考になり得る。例えば、生産ラインに対するサイバー攻撃は事業停止をもたらし得る。これはスマートファクトリーにおいては特に問題となろう。例えば、自動車工場の制御システムがマルウェアに感染してしまうと生産停止という事態が発生してしまう(39)。抽象的ではあるが、この点を刑法の観点から考えてみると、表1では「限定範囲での」事業停止と「広範囲での」事業停止とを影響レベルの観点から分けて認識している点から一定の示唆が得られるかもしれない。既に刑法上、電子計算機損壊等業務妨害罪がシステムのネットワーク化を踏まえて通常の偽計又は威力業務妨害罪よりも重いものとして法定されているが(この点については後述第3章第3節第3款参照)、事業停止の範囲について、業務妨害罪は区別していない。影響が生じる範囲の程度の具体化は必要であるが、通常の業務妨害罪よりも法定刑を加重する業務妨害罪があるべきだ、という立論につながるかもしれない。

第3款　得られる示唆

以上を踏まえると、CPSの保護に関しては、情報セキュリティと同様の保護をしつつ、それに上乗せする形での強固な保護が求められている。そのような強固な保護が(少なくとも政策的に)必要であることを正当化する理由として、表1における種々のフィジカルへの悪影響があると考えられ、既存の法規制を精査しつつ、あり得べき法状態を検討して

(39)　佐々木・前掲注(4)59頁。

いく必要がある。

第３節　小括

以上、制御システムや重要インフラが互いにネットワークを介してつながることにより、利便性が提供されつつも、これらに対するセキュリティ維持をどう図るかが、極めて重要な問題として意識されていることがわかる。ネットワーク化は、我々の生活、企業活動を効率化してくれたが、同時に、ネットワーク技術へのますますの依存をも意味し、サイバーセキュリティ対策を考慮しなければならないことをも意味する(40)。こうした動向を踏まえ、第３章において、刑法学からどのようなアプローチができるか、を考えていきたい。

第３章　CPSの保護とサイバー犯罪対策立法

第１節　議論の前提

本研究では、既に一定のCPSを守るための枠組みが機能しているにもかかわらず、攻撃者が、未発見の、あるいは発見されて間もない脆弱性を突く等してハッキングやクラッキングを行い、その結果、フィジカル面での状態の変更を通して、重要インフラや法人の業務、及び市民の生活に重大な支障が生じる場合を想定している。

サイバー攻撃による弊害の中でも一定のものはここでの研究対象とはならない。例えば①データを変更等することによって他人の財産状態への侵害(財産的損害を与える行為、より広く捉えれば金融に影響を与える当罰的行為)や②他人にデータを送信することによってデータの内容を見聞きした人へ精神面への悪しき働きかけ(いじめ(41)や脅迫)を行う場合(精神面での法益侵害を目的とする当罰的行為)は除かれる。これらには「データ処理に不可避的に伴う事柄以外の正常でないシステムの物理的挙動」

---

(40)　藤原健太「PAへのサイバー攻撃の脅威」計装61巻11号28頁(2018)。

(41)　いじめの犯罪化については、別途、研究を進めている。西貝吉晃「アメリカにおけるサイバーいじめ対策立法の刑法的側面」日本法学85巻４号410頁(2020)。

が欠けるからである。

厳密にいえば、データの変更も磁性体の状態が変わっているから「フィジカル」だといえなくもない。しかし、本研究で明らかにしたいのは、現実世界で起こる事象を表現したデータを処理するシステムである(42)、例えば、コネクティッドカーや航空機のシステムをハッキングしてそれらの制御を奪う行為や発電所のコンピュータの制御を乗っ取る行為の当罰性の有無及び程度や処罰方法論である。それゆえに「データ処理に不可避的に伴う事柄」の変更を除いている。

そこで、データ処理によって行われる物理的なシステムの挙動の安全を法的に図る方法を考えることを対象に研究を行っていく。既に1980年代のコンピュータ犯罪対策立法の際の議論において、コンピュータの破壊という物理的事象に対してさえ、社会システムが大幅にコンピュータに依存している現状(1980年代当時)において、コンピュータの破壊は単にものが壊されることを越えた意味を有する(43)、とか、物が壊されることについて器物損壊罪で対応できるかもしれないがそれによって起こる社会の混乱について適切な法定刑で処罰できるかが問題になる(44)、といった指摘がなされていた。当時は、コンピュータという物の損壊を器物損壊罪で捕捉するだけでは足りないという問題意識だったのであろう。しかし、コンピュータは、今や知的作業を代替するだけにとどまらない。センサ技術やロボティクス技術の進歩により、物理的労力もが代替されるだろう。代替するだけにとどまらず、先進的な技術は一部において人間の認知や行動能力を上回るから、人間により豊かな生活環境を与えてくれるであろう(45)。もっとも、そうしたシステムが物理世界で暴走したら取り返しのつかない損害が生じるかもしれない。現在の技術的状況はCPSのセキュリティを刑法の観点から考える必要性を教えてくれる。

---

(42) 中島・前掲注(19)238頁。

(43) 大谷實＝古田佑紀＝西田典之「〔鼎談〕コンピュータ犯罪と刑事立法の課題」ジュリ846号16頁、28頁(1985)〔西田典之発言〕。

(44) 大谷ほか・前掲注(43)28頁〔古田佑紀発言〕。

(45) Society5.0における新たなガバナンスモデル研究会・前掲注(3)2.4以下。

同時にCPSの利用者側のセキュリティ対策が一定程度行われていることを前提としても、システムの脆弱性を突かれることは避けがたいことから、その点を法規制で一定程度抑止する必要がある（技術と法律の協働によるセキュリティ対策[46]）。とりわけ、CPSに対する攻撃が問題になる場合、フィジカル面での悪影響が甚大になるおそれがあり、必要に応じて刑法的規制を用いて、一定の抑止効果を期待することが重要になってくる。

第２節　サイバー→フィジカル→社会的悪影響というモデルに対する法的アプローチ

サイバー攻撃によって生じるフィジカル面での弊害の分析方法について、今一度、第２章第１節第１款で紹介した経済産業省のサイバー・フィジカル・セキュリティ対策フレームワークをみてみると、そこでは

①サイバー空間における侵害⇒

②フィジカル空間における実質的[47]変化⇒

③（①ないし②から派生して生じる）社会的な悪影響

の３段階に分けた考察がなされている。例えば、経済産業省のビルガイドラインは、セキュリティサイドの議論として、「ビルシステムが攻撃を受けることで考えられる最も大きな影響は、ビルのサービスが停止し、その結果として入居者の業務が停止ないしは著しく影響をうけることである。これはビルとしての業務が妨害され、社会的信用の棄損につながるだけでなく、顧客への補償などの金銭被害や顧客離れ等の二次被害へと広がる可能性も考えらえる」[48]とする。

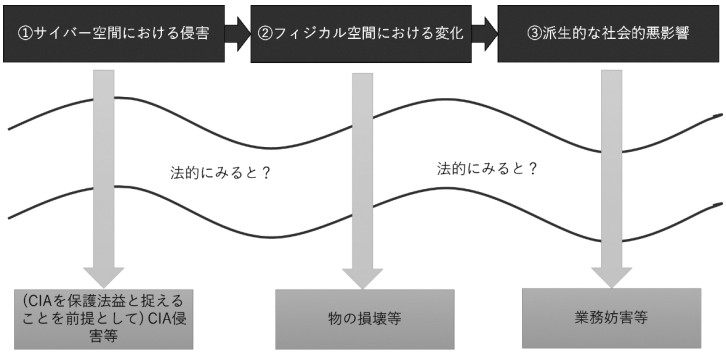
もっとも、事実的な考察軸である①、②と社会的評価という考察軸である③とが連続的に並んでいることについては法的な見地からは説明を

⑷⑹　西貝吉晃『サイバーセキュリティと刑法』28頁（有斐閣、2020）。

⑷⑺　第１節で述べたところに従い、サイバー空間によるデータ変更によって不可避的に伴うものを除く趣旨。

⑷⑻　経済産業省 産業サイバーセキュリティ研究会 ワーキンググループ１（制度・技術・標準化）ビルサブワーキンググループ「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第１版」16–17頁（2020）。

図６　サイバー・フィジカル・セキュリティの法的考察のための３つのレイヤー



それぞれのレイヤーにおける事象自体から法益侵害と評価できる場合がある

要する。

まず、①や②について社会的悪影響の有無の観点から独立の評価を行うことは可能である(図６の①または②から下に出ている矢印参照)。すなわち、①についていえば、データを無権限で閲覧されない利益(機密性)、無権限で変更されない利益(完全性)、利用したいときに利用できる利益(可用性)はサイバーセキュリティ(情報セキュリティ)そのものであって、一定程度、法的にも保護され得る。刑法学においても、例えば機密性を直接保護する罪として(電気)通信の秘密侵害罪(電気通信事業法、有線電気通信法、電波法)がある。

次に、人を殺せば殺人罪になる、というように、②で問題とする物理的事象そのものからも、言い換えれば②についての攻撃によって生じる③の側面での新たな妨害や権利侵害等を認定せずとも、固有の法益侵害(刑法上保護すべき利益の侵害)やその危険の発生を認めることが可能である。器物損壊罪が業務妨害罪等と別に存在していることからも同様のことがいえる。

さらに、器物損壊のような犯罪を手段として威力業務妨害罪が成立することがあり得る。法律は②(人に対する偽計や威力の行使)を類型化しつつ、③(業務の妨害)を考察していた。③は、②から③が生じるという意

味で、②だけをみて発見される法益侵害とは異なるものである。つまり、③でいう社会的な悪影響というのは、①や②それ自体や①⇒②の過程を社会的に評価するだけでは評価しきれないもののことをいうものと考えられる。上記で例示したとおり、刑法上は例えば信用の毀損や業務の妨害等が③にあたる。民法上のプライバシー侵害もこのレイヤーに含まれ得る。さらにレピュテーションの侵害や(例えば文化財が焼失するという事態が生じれば)無形的価値の減少も考えられよう(図６でいえば③の下に位置づけられる法益侵害)。

第３節　サイバー犯罪対策立法の現状

第１款　総説

第２節の議論を踏まえると、CPSのサイバー攻撃からの法的な保護を考える際には、サイバー空間の保護を目的とした「サイバー犯罪対策規定」と「フィジカル空間の保護を目的とした伝統的犯罪」とを区別して分析しつつ、その融合を図れないか、検討していくのがよい、と考える。議論の軸を整理することにより、法益侵害の重大性や捕捉範囲をある程度の方向性をもって定めることを期待できるほか、サイバー・フィジカル・セキュリティの議論との対応がとりやすくなることも期待できる。そこで本節では、まず、サイバー犯罪対策立法の現状について整理する。ここではデータやプログラムの保護の方法が主に問題になるが、その延長線上でサイバー・フィジカル・セキュリティがどのように保護されているかを探ることになる。

第２款　サイバー⇒フィジカルという因果過程の存在

まず、ここでは、サイバー空間への攻撃によってフィジカル空間への悪影響が出る、という意味での因果過程の認識が重要である。

サイバー空間における行為について、フィジカル空間において同じ行動を採った場合に処罰されるだろうか？というアナロジーで説明されることがある。これは、ここでいう因果過程の問題とは別であることを指摘しておきたい。このアナロジーは、サイバー空間に存在する情報やデータの保護のためにフィジカル空間における法律論を流用できないか？という理解に基づいている。例えば、不正アクセス罪を考える際に住居侵入罪のアナロジーを用いる考え方やわいせつなデータをダウン

ロードが可能なウェブページを自動販売機に例える考え方がそれである。この種のアプローチに効用があるとすれば、サイバー空間内で直接発生した法益侵害が完結する(派生して生じる社会的評価の毀損等は含まない)場合である。しかし、サイバー・フィジカル・セキュリティの維持に関する法律論の場面ではそうした考慮をすべきではないと考える。

つまり、サイバー・フィジカル・セキュリティにおいては、いわばサイバー空間とフィジカル空間の２つの干渉し合っている世界が存在することを前提に、世界間のインタラクション(CPSFでいうところの「転写」の概念)の態様を理解する必要がある。フィジカル空間の事象がセンサ系によってデータ化されることでサイバー空間におけるデータ処理に影響が生じ得るし、サイバー空間のデータ処理の結果がフィジカル空間に影響を与えることになる。法的思考を行う上でも、相互干渉が問題となる。

こうしたことを正面から考慮できるアプローチは、既に用意されているフィジカル空間用の刑罰規定(公共危険犯等)とサイバー空間用の刑罰規定(サイバー犯罪対策立法)のそれぞれの存在をまず認識し、 その上で、サイバー・フィジカル・セキュリティの観点から抑止したい行為類型がある場合に、それらの規定群を拡張的に立法することで対応すべきなのか？それとも、独立の法益侵害を肯定すべきなのか？といった事柄を正面から考察する方法論だと考えられる。

CPSへの攻撃は、ICTを用いて行われることで、場所を選ばず、準備さえしておけばワンクリックで実行可能なうえに、広範囲に影響を与え得る。その意味では、この攻撃は「サイバー犯罪」の特徴を持っている。同時に、結局、問題となっているのが人の生命・身体それ自体の侵害やこれに対する危険も含めたものなのであれば、伝統的なフィジカル面における犯罪の法益論を借用することも合理的である。こうした特徴を「サイバー・フィジカル・セキュリティ侵害の両面性」と呼んでおきたい。

こうした両面性を踏まえて、現状のサイバー犯罪対策規定の特徴を考える。1980年代のコンピュータ犯罪対策立法当時においては、既にデータの変更等により、電子計算機使用詐欺であれば財産状態の変動、電子計算機損壊等業務妨害であれば業務の妨害といった、一定の法益侵害が

肯定される類型については対処がなされた。当時は情報処理の結果としてのフィジカル空間への大きなダメージを主として考察する必要がなかったし、現実に、プラントの操業を停止させるような攻撃を加えることを想定する必要は大きくはなかった。これに対し、現在では、フィジカル空間の状態維持という視点を踏まえて、各犯罪類型の限界を探る必要がある。

第３款　電子計算機損壊等業務妨害罪を中心としたサイバー犯罪対策規定の検討

第１項　総説

本章第２節で紹介した３つのレイヤーを再掲する。

①サイバー空間における侵害⇒

②フィジカル空間における実質的変化⇒

③(①ないし②から派生して生じる)社会的な悪影響

サイバー犯罪対策規定には、①に関連する犯罪類型、つまり①のみ、①⇒③、及び①⇒②⇒③といった、サイバー空間の状態の変更に基づいた議論が可能になる点で、一定の有用性が期待され得る。

①に着目しているサイバーセキュリティに関する犯罪(CIA犯罪)には、不正アクセス禁止法上の不正アクセス罪やデータの不正作出(電磁的記録不正作出罪)や不正変更(私用電磁的記録毀棄等)があり得る。 これらは、③ではなく、①に対して直接に当罰的か否かという社会的評価を行ったものだといえる。CIAとの関係で考えてみると、例えば電磁的記録の不正作出や不正変更により権限に基づいて作成されたデータの完全性や可用性が失われるから、既に一定程度、刑法上の犯罪類型でIAの保護が達成されている。もっとも、CPSの保護を考える際には、一般的に電磁的記録の損壊等を行為態様に入れ、かつ③のレイヤーを結果要件に含めている電子計算機損壊等業務妨害罪を主な検討対象にするのがよい、と考える。

そこで、電子計算機損壊等業務妨害罪をメインの考察対象として捉えつつ、その前に、不正指令電磁的記録供用罪、及び不正アクセス罪について簡潔に、本稿の目的と関連する限りで考察を行いたい。

第２項　不正指令電磁的記録供用罪

本稿の冒頭で述べた事例からわかるように、マルウェアを投入することにより重要インフラの運行が停止する危険がある。この場合、マルウェアを投入したこと自体を捉えて、不正指令電磁的記録供用罪（刑法168条の２第２項）の成否を論じる余地がある。

不正指令電磁的記録に関する罪の保護法益は、電子計算機のプログラムが、電子計算機に対してその使用者の意図に沿うべき動作をさせず、またはその意図に反する動作をさせるべき不正な指令を与えるものでないという社会一般の者の信頼、要約すれば、電子計算機のプログラムに対する社会一般の者の信頼だと解されている(49)。

供用の客体である不正指令電磁的記録には、マルウェア全般が優に入るほど、同概念は広く解され得る。コンピュータ・ウィルス、トロイの木馬、ワーム、スパイウェアも、条文上の要件（重要になるのは反意図性及び不正性）を充たすものであれば不正指令電磁的記録にあたる(50)。

そして、不正指令電磁的記録の「供用」とは、不正指令電磁的記録を「電子計算機の使用者にはこれを実行しようとする意思がないのに実行され得る状態に置くこと」だとされる(51)。実際にプログラムが実行された場合には、それ以前に実行され得る状態に置かれたといえるから、当然に供用にあたる。手段の限定はない、と解される。例えば、メール添

---

(49)　大塚仁＝河上和雄＝中山善房＝古田佑紀編『大コンメンタール刑法 第３版 第８巻』341頁〔吉田雅之〕（青林書院、2014）（以下『大コンメンタール刑法 第３版 第８巻』として引用）。もっとも、その理解自体に疑問はあり、不正指令電磁的記録に関する罪は、サイバーセキュリティ（CIA）を保護する罪として捉えられるべきだと考える（本罪の解釈論については、西貝吉晃「技術と法の共進化を企図した法解釈の実践」法セミ792号40頁（2020）、西貝吉晃「不正指令電磁的記録に関する罪の解釈論」罪と罰58巻３号20頁（2021）を参照されたい）。ただし、私見のように捉えたとしても、サイバー・フィジカル・セキュリティの議論はサイバーセキュリティ＋α（安全性）なのだから、本文で述べるような、犯罪結果のフィジカル面に着目して議論を掘り下げるべきだという主張は依然として成立する。

(50)　『大コンメンタール刑法 第３版 第８巻』344頁〔吉田雅之〕。

(51)　『大コンメンタール刑法 第３版 第８巻』349頁〔吉田雅之〕。

付(メールサーバへのアップロード)やウェブサイトへのアップロードを行い、情を知らない第三者にダウンロードさせることや、CD-R等の有形的な媒体を交付し、情を知らない第三者に起動中のPCに当該CD-Rを挿入させて、その中に保存されているプログラムを実行可能な状態に置くこと等が考えられる(52)。

上記のように実行され「得」る状態で既に既遂に達するにもかかわらず、供用罪は未遂犯をも処罰することに注意しておきたい。それゆえ、上記の例のうち、情を知らない第三者がダウンロードしなかった場合においては、既遂犯は成立しないものの、未遂犯が成立し得る。この場合、未遂犯の成否は、情を知らない第三者が、問題となるファイルをダウンロードする蓋然性の程度に依存すると解される。例えば、メール添付に関してはメールサーバへのアップロード時に未遂犯が成立し、ウェブへのアップロードについては個別事案によるが、アップロード時点で未遂犯が成立する場合もあると解されている(53)。

こうしてみると、サイバー・フィジカル・セキュリティの保護の文脈においても、その侵害は主にプログラムの異常な挙動、あるいは突然の停止に基づくものであるから、いわゆるマルウェアが使用された場合には、多くの場合、本罪が成立する。

もっとも、不正指令電磁的記録供用罪は、既に述べたとおり、ソフトウェア(プログラム)の挙動に対する社会的信頼を保護する罪として立法され、これは①のレベルのものにとどまるもの、すなわち②、③のレイヤーにおける侵害を考慮して立法がなされているとは言いがたい、言い換えれば②、③を考慮して法定刑が設定されていないともいい得る。つまり、本罪をCPSの物理的挙動に対する社会的信頼をも保護する罪として捉えることはできず、本罪が成立するからCPSの保護が万全であるとはいえないと思われる。また、CPSに対する攻撃がマルウェアの投入以外の態様で行われることもあり得るから、本罪の成否を集中して考察することも、方法論としては適切ではない。

---

(52) 『大コンメンタール刑法 第３版 第８巻』349頁-350頁〔吉田雅之〕。
(53) 『大コンメンタール刑法 第３版 第８巻』353頁〔吉田雅之〕。

第３項　不正アクセス罪

そこで、次に不正アクセス禁止法上の不正アクセス罪(不正アクセス行為の禁止等に関する法律11条、３条)を検討する。

不正アクセス罪は、ユーザ(利用権者)認証システムに対して、他人の識別符号を入力し、あるいはセキュリティ・ホールを突くコードを入力することによって、その認証機能を突破して、それを突破しないとできない態様での利用を可能にする行為を処罰する。同罪については、CIAのうち、どの部分を保護しているかにつき、学説上の争いもあり比較法的にも議論が多い。不正アクセス罪の捕捉範囲の特殊性は、CPSの保護にどこまで不正アクセス罪が利用可能か、という問題を解く際の鍵ともなる。

不正アクセス罪の規定自体は複雑であるが、まず明らかなのは、サイバーセキュリティにおいて議論されている脆弱性を突く攻撃全てが不正アクセス罪に該当するわけではない、ということである。技術的にユーザ認証機能が存在しなければならず、現実に各ユーザの識別を行える状態になっていなければならないゆえに、ユーザIDとパスワードを付与しているといっても、利用権者が一人の場合には同罪を適用できない。これが本罪をネットワーク上での円滑なコミュニケーションを維持する罪だと構成し得る所以であるが、それは同時に、本罪がフィジカル面での悪影響に焦点をあててつくられてはいない罪であることをも意味している。

また、アクセス管理者の行為は不正アクセス禁止法では絶対に処罰されない。アクセス管理者はいわば当該ネットワークにおける「(全権限を有する)神」といってもよく、それにはサイバーセキュリティの維持向上の観点からは一定の理由があるとは思われる(54)。もっとも、そのような神が、フィジカル面への大事故を惹起させるような「悪魔」になる場合も同法では処罰できない。例えば、管理者が権限濫用的な指令を送って、フィジカルシステムに一定の挙動をさせて、死傷事故を発生させても、それは広い意味では「不正アクセス」かもしれないが、我が国

---

(54)　西貝・前掲注(46)247頁以下。

の不正アクセス禁止法上の不正アクセス行為ではなく、不正アクセス「罪」では処罰できない。さらに、認証機能しか保護しないため、正当に認証された利用権者の利用権の濫用的な行為にも使えない。コンピュータ・システム(CPS)の制御を掌握した時点で処罰可能にする不正アクセス禁止法上の不正アクセス罪は、処罰の「時点」の観点からするとCPSの万全な保護の観点からは妥当かもしれないが、アクセス管理者や利用権者といった「内部者」による権限濫用行為を処罰しにくい。CPSの保護に直接的に使う上で、同罪にはCPSの保護とは関係ない観点からの限定がかけられている可能性がある。

この点はサイバー・フィジカル・セキュリティを保護する際には大きな問題となる。予想される攻撃者(行為者)としては外部者だけでなく(平時にCPSの制御について一定の権限を有している)内部者も考えておくべきである。なぜなら、その場合の内部者は、外部者よりも既に多くの制御が可能な状態にあるから、より容易に、物理的な危険を発生させ得るとも考えられる上、そのような内部者にはむしろ、安全を維持すべき業務上の義務が肯定されると評価することも可能に思われるからである。

第４項　電子計算機損壊等業務妨害罪

そこで検討すべきなのが、電子計算機損壊等業務妨害罪(刑法234条の２)である。この罪は、データの改変や消去を通し、システムに異常動作をさせて業務を妨害する行為等、いわばクラッキングを処罰する規定である。

本罪に関しては、そもそも行為態様に電子計算機(コンピュータ)の物理的損壊が含まれているからか、立法当時から、温度、湿度を急激に上昇下降させることによる物理的な動作環境の破壊[55]による業務妨害行為も挙げられていた。また、重要インフラに相当するシステムが攻撃されることも考慮されていた[56]。これはサイバー・フィジカル・セキュリ

55　米澤慶治編『刑法等一部改正法の解説』102頁〔横畠裕介〕(立花書房、1988)、大塚仁＝河上和雄＝中山善房＝古田佑紀編『大コンメンタール刑法 第３版 第12巻』250頁〔鶴田六郎＝河村博〕(青林書院、2019)(以下『大コンメンタール刑法 第３版 第12巻』として引用)。

ティ侵害の一例だといえ、データ処理を介してこうした状況を作出した場合、①⇒②⇒③の因果過程を経ている。サイバー空間上のデータを変更等し(①)、フィジカル空間に悪影響を与え(②)、さらにこれによって法益侵害を惹起する(③)場合を捕捉している点で、電子計算機損壊等業務妨害罪は、本研究における考察対象として重要な犯罪である。

もっとも、行為態様としては、①(サイバー)⇒③(社会的な悪影響)のようにフィジカルを介さない場合だけでなく、データ処理と関係のない②(フィジカル)⇒③(社会的な悪影響)の場合をも捕捉している。電子計算機それ自体を物理的に損壊する行為(ハンマーで壊す行為)によって業務を妨害した場合にも本罪が成立する。これは②⇒③、つまり伝統的な犯罪類型(器物損壊罪)について業務妨害罪の要素を加えて加重したものと評価できよう[57]。一方で、本罪は同時にデータの変更(電磁的記録の損壊)を介して業務を妨害すれば足りるから、データを変更、消去したりして、業務を妨害する①⇒③の類型という意味で、②には着目していない場合も捕捉する。その意味では、複雑な行為態様について精査が必要である。

また、本罪は業務妨害罪の一類型だが、業務妨害罪の類型には既に偽計・威力業務妨害罪が存在していた。広汎な業務が電子情報処理組織による自動的な処理によって行われるようになり、これに対する業務妨害行為が従来に比して重大な業務妨害につながり得ること、及びこれが間接的に国民生活に大きな影響を及ぼし得ることに鑑み、他の業務妨害罪に比して重い法定刑を持つ規定が必要になったことから本罪が新設された[58]。

⑸⑹　加藤晃久＝相浦勇二＝小高隆雄「刑法等の一部を改正する法律について」警察公論42巻９号56頁、66頁(1987)は航空管制制御システム、原子力発電制御システム、ダム水量管理システム、交通管制システム、銀行業務総合オンラインシステム、乗車券発売予約システムを挙げていた。

⑸⑺　本罪がないと、器物損壊罪のみか、せいぜい器物損壊罪と威力業務妨害罪の観念的競合になるにとどまり処断刑の上限が３年であったところ、電子計算機損壊業務妨害行為として上限５年の法定刑を有する一罪とした点に意味がある。

本罪は電子計算機や電磁的記録を客体とする罪であり、偽計・威力業務妨害罪は人を客体とする罪だと捉えることも可能であるが[59]、そもそも偽計・威力業務妨害罪も物を客体とした行為について成立し得るから[60]明確な峻別は難しい[61]。

サイバー・フィジカル・セキュリティの保護の観点を踏まえつつ、本罪の要件解釈を確認し、その上で、本罪の機能をまとめたい。本罪は次に示すア、イ、ウの三段階の因果過程を予定する[62]。

ア―1　人の業務に使用する電子計算機／その用に供する電磁的記録[63]　を損壊し、
ア―2　人の業務に使用する電子計算機に　虚偽の情報／不正な指令　を与え、
ア―3　その他の方法により、
　イ　電子計算機に　使用目的に沿うべき動作をさせず、／使用目的に反する動作をさせて、
　ウ　人の業務を妨害した

58　『大コンメンタール刑法 第３版 第12巻』246頁-247頁〔鶴田六郎＝河村博〕。立法直後にはコンピュータを特権化するものだという疑問も呈されていた（神山・前掲注31）33頁以下）。

59　西田典之「コンピュータと業務妨害・財産罪」刑法雑誌28巻４号49頁（1988）。加藤＝相浦＝小高・前掲注56）67頁。

60　このように解すると、電子計算機損壊等業務妨害罪は、処罰の欠缺を埋めるためのものではなく、従前の業務妨害罪の加重類型となる（松原芳博『刑法各論 第２版』170頁-171頁（日本評論社、2021）、内海朋子「判批」成瀬幸典＝安田拓人＝島田聡一郎編『判例プラクティス刑法Ⅱ各論』142頁（2012）。特段断りなく加重犯だとするものに団藤重光『刑法各論綱要 第３版』690頁（創文社、1990））。データの不正操作も、（人が正常な業務の遂行が可能と合理的に期待している場合にその遂行を妨げる計略を用いることと解される）「偽計」にあたると考えるべきだとするものに的場純男「コンピュータ犯罪に関する刑事法上の問題点―主として立法的観点から」ジュリ846号６頁、12頁（1985）、板倉宏「情報犯罪と刑事法」警察学論集40巻４号109頁、121頁（1987）。

なお、本罪は、ネットワーク化の進展に伴い、偽計・威力業務妨害罪とは異なって、2012年に未遂犯が導入され、処罰が早期化された。

第１目　保護法益

本罪は個人的法益に対する罪であり[64]（ただし後述第２目⑵の議論も参照）、その保護法益は人の社会的・経済的活動たる（コンピュータ化された）業務遂行の安全[65]と解されている。業務については次で述べる。

第２目　業務の妨害㋒

⑴　罪質

本罪は業務妨害罪の一類型であり、人の業務を妨害した場合に処罰範囲が限定される。ここでは、威力業務妨害罪（刑法234条）において重要な論点であった、強制力のある公務が同罪で保護対象となる業務から除かれる、という議論については、反対説はあるが[66]、電子計算機による情報処理それ自体は権力的なものとはいえないから[67]、本罪では問題に

61　双方の構成要件に該当するような事案において、結果が一つの場合には、法条競合（特別関係）にたつと解することが可能である。

62　『大コンメンタール刑法 第３版 第12巻』247頁〔鶴田六郎＝河村博〕。

63　業務に使用される電子計算機の用に供する電磁的記録（『大コンメンタール刑法 第３版 第12巻』249頁〔鶴田六郎＝河村博〕）。

64　『大コンメンタール刑法 第３版 第12巻』247頁〔鶴田六郎＝河村博〕、岡村久道『情報セキュリティの法律 改訂版』241頁（商事法務、2011）。

65　米澤編・前掲注55）97頁〔横畠裕介〕、『大コンメンタール刑法 第３版 第12巻』247頁〔鶴田六郎＝河村博〕、大谷實「コンピュータ関連犯罪と刑法の一部改正（下）」判タ651号28頁、29頁（1988）。電子計算機を介して行われる人の業務が保護される（前田雅英編『条解刑法 第４版』726頁（2020））。

66　佐伯仁志「【刑法各論の考え方・楽しみ方】〔８〕業務妨害罪」法教363号83頁、87頁（2010）は、強制力を行使する権力的公務としてコンピュータを用いた警察による通信傍受を挙げ、海賊船を追跡中のイージス艦のコンピュータに対するサイバー攻撃について、電子計算機損壊等業務妨害罪の成立を認めることには違和感があり、業務性を否定することにより処罰の間隙が発生するのであれば、電子計算機損壊等公務執行妨害罪の新設が妥当だとする。

67　西田典之〔橋爪隆補訂〕『刑法各論 第７版』144頁（弘文堂、2018）。

ならない、とされている。つまり、業務が公務としてなされていると否とを問わず、人が反復継続して行う社会的活動全般が本罪での保護対象となる業務にあたる[68]。業務の限界については、偽計・威力業務妨害罪における業務についての議論が援用されるべきであり、個人が娯楽のために開設したHPの内容の改変では業務妨害につながらない（本罪は不成立）[69]。

重要インフラに関していえば、官民関わらずその多くが、端的に電子計算機損壊等業務妨害罪における業務に含まれる、と評価できる。一方で、娯楽等の専ら私的な用途にしか使っていないCPS（IoT）に関しては、本罪の保護が不可能になるところ、この点は立法論としてはなお議論が必要だと思われる。

本罪については侵害犯説[70]も有力であるが、一般的には危険犯だと解されており、妨害の危険の発生により成立する[71]。現実に人の業務を妨害する必要はない[72]。また、具体的危険犯説も有力であるが[73]、他の業務妨害罪と同様に解するのであれば、抽象的危険犯だということになろう[74]。

⑹⑻　『大コンメンタール刑法 第３版 第12巻』172頁〔佐々木正輝〕、『大コンメンタール刑法 第３版 第12巻』248頁〔鶴田六郎＝河村博〕。

⑹⑼　宇賀克也＝長谷部恭男編『情報法』254頁〔佐伯仁志〕（有斐閣、2012）、斎野彦弥「判批」佐々木史朗編『判例経済刑法大系 第３巻』413頁、414頁（2000）、内海朋子「判批」成瀬幸典＝安田拓人＝島田聡一郎編『判例プラクティス刑法Ⅱ各論』143頁（2012）。

⑺⑽　西田〔橋爪補訂〕・前掲注⑹⑺145頁、山口厚『刑法各論 第２版』168頁（有斐閣、2010）、山中敬一『刑法各論 第３版』248頁（成文堂、2015）、松原・前掲注⑹⑽171頁、170頁、佐伯・前掲注⑹⑹90頁、浅田和茂『刑法各論』177頁（成文堂、2020）。

⑺⑴　西田・前掲注⑸⑼51頁。未遂犯を処罰する危険犯もあるから、本罪が未遂を処罰することをもって侵害犯だと解すべきだという主張は難しい（ただし、渡邊卓也「判批」長谷部恭男＝山口いつ子＝宍戸常寿『メディア判例百選 第２版』246頁、247頁（2018））。

⑺⑵　米澤編・前掲注⑸⑸98頁〔横畠裕介〕、前田雅英編『条解刑法 第４版』726頁。

⑺⑶　大塚仁『刑法概説（各論）第３版増補板』166頁（有斐閣、2005）。

(2) 加重根拠論

電子計算機損壊等業務妨害罪は、コンピュータに対するクラッキングにより多方面への甚大な被害をもたらすおそれがあることから、公共危険犯的性格を有するとされることがある[75]。この考え方は解釈として、本罪の適用範囲を、電子計算機による業務の妨害の影響が単に一個人、一企業の内部的事務処理にとどまらず、社会公共に対しても被害や混乱を及ぼしうる場合に限定すべきことにもつながることもある[76]。

ただし、解釈論としては、そう解釈するだけの文言上の根拠が乏しく[77]、むしろ法定刑の上限を上げる根拠になったにとどまると解される[78]。一方で、公共危険犯的に理解する考え方からは立法論的な示唆を得ることはできると考える。すなわち、サイバー犯罪がフィジカル面での損害を発生させ、これにより社会の混乱といえるような大規模な業務等の妨害が発生する場合(第２章第２節の「制御システムのセキュリティ」の議論も参照)は、現行の電子計算機損壊等業務妨害罪よりももっと重い

---

74 加藤＝相浦＝小高・前掲注56)69頁。判例の理解(抽象的危険犯)についての観察につき平川宗信『刑法各論』210頁(有斐閣、1995)〔ただし同書は侵害犯説〕、夏井高人「サイバー犯罪の研究(一)」法律論叢85巻１号210頁(2012)〔ただし夏井自身は具体的危険犯説〕。なお、判例を具体的危険犯だと評価するものとして大谷・前掲注65)31頁、大谷實『刑法講義各論 新版第５版』159頁(成文堂、2019)〔ただし同書は侵害犯説。156頁〕。

75 西田・前掲注59)48頁。業務妨害の波及効果が重大だと指摘するものに団藤・前掲注60)690頁。さらに的場・前掲注60)15頁。

76 西田・前掲注59)50頁。被害の重大性を理由に本罪に社会的法益に対する罪の側面を見いだすものに大塚・前掲注73)164頁、井田良『講義刑法学・各論 第２版』202頁(有斐閣、2020)、中森喜彦「コンピュータ犯罪と刑法の一部改正」法教81号89頁、92頁(1987)。

さらに、HP上のデータを書き換えた大阪地判平成９年10月３日判タ980号285頁について、電子計算機損壊等業務妨害罪で加重処罰するに値するほど重大な業務妨害の危険が生じていたか疑問を呈することで、一定の限定解釈を前提としているとみることのできる見解として内海・前掲注60)142頁。

77 宇賀ほか編・前掲注69)251頁-252頁〔佐伯仁志〕。一方で、加重の根拠である結果の重大性の文言が記載されていないことについてやや批判的にみる見解として中森・前掲注76)92頁。

法定刑の加重類型が妥当だといえるかもしれないからである。

第３目　行為(ア)

(1)　行為客体

本罪の行為客体には「人の業務に使用する電子計算機」と業務に使用される電子計算機の用(79)「に供する電磁的記録」がある。

①　「人の業務に使用する電子計算機」

「人の業務に使用する」における人の業務とは、犯人以外の自然人、法人、法人格なき社団等によって行われる、公務を含む、人が反復継続する意図のもとに行う経済的社会的活動のことをいう、と解されている(80)。スタンドアローンのコンピュータも客体に含まれる(81)。実力で業務妨害行為を排除することができないから、権力的な公務というものを想定できず、公務も、ここでいう業務に含まれると解すべきだとされる(82)。

次に「電子計算機」の意義であるが、刑法は電子計算機を定義していない。電子計算機の概念を、自動的にデジタルデータを処理する装置として捉えることも可能である(83)（無限定説）。

しかし、本罪における電子計算機の概念は一定程度限定されて理解さ

---

(78)　大谷・前掲注(65)29頁〔さらに法定刑の下限が変わっていないことを指摘〕、芝原邦爾「コンピュータによる情報処理と業務妨害罪」ジュリ885号11頁、12頁（1987）。さらに堀内捷三「コンピュータ犯罪」芝原邦爾＝堀内捷三＝町野朔＝西田典之編『刑法理論の現代的展開』142頁（日本評論社、1996）も参照。

さらに、軽微な事案にも本罪を適用可能なことについて再考しようとするものに鶴田六郎「判批」警察学論集43巻２号141頁、155頁（1990）。

(79)　『大コンメンタール刑法 第３版 第12巻』249頁〔鶴田六郎＝河村博〕。

(80)　『大コンメンタール刑法 第３版 第12巻』247頁-248頁〔鶴田六郎＝河村博〕、米澤編・前掲注(55)99頁〔横畠裕介〕。

(81)　伊藤渉＝小林憲太郎＝齋藤彰子＝鎮目征樹＝島田聡一郎＝成瀬幸典＝安田拓人『アクチュアル刑法各論』151頁〔島田聡一郎〕（弘文堂、2007）。

(82)　『大コンメンタール刑法 第３版 第12巻』248頁〔鶴田六郎＝河村博〕。

(83)　本罪の解釈論としてではないが、電子計算機の概念の一般論として西貝・前掲注(46)293頁。

れている（限定説、立法担当者及び通説）。限定説の立場からは、人に代替する作業を行うものこそ本罪で捕捉すべきであるから、本罪における電子計算機は、それ自体が自動的に情報処理を行う装置として一定の独立性をもって業務に用いられているもの、すなわちそれ自体が業務を左右するような判断、事務処理、制御等の機能を果たしているものに限定される[84]。

そして、当該機器自体が自動的に情報処理を行う装置とはいえない家電製品、自動カメラ、自動販売機や、一定の情報処理を行ってはいるが、それ自体業務を左右するような判断、事務処理、制御等の機能を果たしていない電卓、電子手帳、電子辞書は、電子計算機にあたらない、と解されている[85]。

電子計算機の概念自体をこのように限定する背後には、他の業務妨害罪よりも重い法定刑を有する電子計算機損壊等業務妨害罪の違法を基礎づけるだけの結果を発生させる原因となるある程度高度なデータ処理を行っているものに客体が限定されるべきだという考慮がある。例えば、パチンコ遊戯台上の電子計算機である主基板について、あらかじめ定められた一定の条件が発生すれば、ロムに読み込まれているとおりの動作をさせる制御機能が与えられているにとどまり、その内容も比較的単純なもので、制御の及ぶ範囲も当該のパチンコ遊技台にとどまり、パチンコ営業に関する情報処理を行うものに過ぎず、結局、自動販売機の電子計算機部分と同様に、個々のパチンコ遊技台の機能を向上させる部品の役割を果たしているにすぎないと認められるから、「業務に使用する電子計算機」にあたらないとした裁判例がある[86]。

以上の考え方は、表２のうち、基本的に①の場合のみを捕捉するものだとも理解できる。

①に限定する考え方につき、学説上は、妥当だと評価されているか、

---

84 『大コンメンタール刑法 第３版 第12巻』248頁〔鶴田六郎＝河村博〕、福岡高判平成12年９月21日判時1731号131頁。

85 『大コンメンタール刑法 第３版 第12巻』248頁〔鶴田六郎＝河村博〕。

86 福岡高判平成12年９月21日判時1731号131頁。

表２　電子計算機損壊等業務妨害罪で問題となる電子計算機の行う情報処理の類型

	高度な情報処理	左記以外（単純な処理）
情報処理が業務に使われる	①	②
上記以外	③	④

同様の解釈がなされるのが一般である[87]。しかし、IoT時代になってスタンドアローンの（ネットワークに接続されていない）電子機器が少なくなってきており、また家電一つとってみても、多機能なものが多くなってきている。これを踏まえると、少なくとも、高度な情報処理を行っていないものの方が少ないとも評価し得る[88]。すなわち、②や④にあたるものが事実上少なくなってきている。

一方で、情報処理の高度性とは独立に、その情報処理の結果が業務に使われているのか否かという観点では、高度な情報処理も専ら娯楽に使われることもあるから（③の類型）、本罪での捕捉は難しいとも解し得る。しかし、業務妨害的な要素を離れてみると、業務に使われているからではなく、情報処理の内容が高度であることによって生じ得る損害が類型的に大きくなる、と考えられる。そうすると、電子計算機の概念を（解釈で）限定することに意味があるのか、疑問が生じてくる。クラッキングを犯罪化する際の立法論として、「業務妨害」の要件がなぜ存在するのか、ということを再考してもよいかもしれない。つまり、クラッキング罪の立法論を考える際には、③も捕捉すべきではないか、という問題意識があってもよいと考えるわけである。

②　その用に供する電磁的記録

損壊の客体となる「その用に供する電磁的記録」とは、業務に使用される電子計算機の用「に供する電磁的記録」だと解されている[89]。業務

87　大塚・前掲注73）164頁−165頁、浅田和茂＝井田良『新基本法コンメンタール　第２版』510頁〔森永真綱〕（日本評論社、2017）等。

88　同様の問題意識をもつものとして岡村・前掲注64）243頁。

に使用されていないバックアップコピーは本罪の電磁的記録からは除外される(90)、とされる。バックアップコピーのデータを使ったデータ処理への(直接的な)影響がないという観点からは正当化され得る。

(2) 行為態様

電子計算機使用詐欺罪と異なり、行為態様に「その他の方法により」があるので、かなりの程度、包括的な捕捉がなされる。

① ア―1 損壊類型

損壊類型には、例えば当該デバイスを別用途にも使えなくなるような物理的な破壊に伴ってデータ処理の不全を惹起するデバイス損壊類型(91)(物理的な加害)と、上記のような物理的な破壊があるとは必ずしもいえない状況の下で行われるデータの消去等のデータ損壊類型(92)(論理的な加害)がある(データ損壊類型があるゆえにこの類型を器物損壊の類型と呼ぶ(93)のはやや語弊がある)。ホームページ上のデータを無権限で書き換える行為は電磁的記録の損壊にあたる(94)。データ損壊類型について、隠匿が含まれるかには問題がある、ともされるが(95)、電磁的記録の隠匿に

---

(89) 『大コンメンタール刑法 第３版 第12巻』249頁〔鶴田六郎＝河村博〕。

(90) 『大コンメンタール刑法 第３版 第12巻』249頁〔鶴田六郎＝河村博〕。ただし、保存用のバックアップコピーの損壊について、中間結果の発生がないことを理由に本罪の成立を認めない見解もある(芝原・前掲注(78)14頁)。

(91) 山口地裁徳山支判平成元年８月10日警察学論集43巻２号141頁。

(92) コンピュータ制御式旋盤機内のプログラムを消去または改ざんし(電磁的記録の損壊)、プログラムによる各旋盤機の自動稼働を不能にして(動作阻害)、製品製造業務を妨害した事例(京都地裁峰山支判平成２年３月26日最高裁判所事務総局刑事局監修『カード犯罪・コンピュータ犯罪裁判例集』218頁)。

(93) 西田〔橋爪補訂〕・前掲注(67)144頁。データ損壊も器物損壊にあたるから、器物損壊の類型と呼んでいるのかもしれないが、データ損壊と器物損壊の法益侵害のあり得る質的な差異をひっくるめて理解しようとしている点に疑問がある。電磁的記録の損壊をも「物理的」加害と捉える米澤編・前掲注(55)97頁〔横畠裕介〕も、物理的の文言はハード面の損壊(本文のデバイス損壊類型)を想起させるから、ミスリーディングである。

(94) 大阪地判平成９年10月３日判タ980号285頁。

よって、その利用を妨げる行為も含まれる、とする考え方もある(96)。さらに検討を要し得る点であるが、データの隠匿により被害者がデータを発見できなくて(人が)困る場合と、データの隠匿(場所の移動)により隠匿されたデータをデータ処理プロセスで読み込むことができずにデータ処理が滞る場合のうち、少なくとも後者は捕捉されると考えれば、比較法的な確認を行っておくべき事柄ではあるが、そうした隠匿も損壊に含めてよさそうである。

デバイス損壊類型についてはフィジカル面に着目して、フィジカルでの侵害の結果、業務上のデータ処理への悪影響を考慮して、動作阻害(イ)を考察するのに対し、データ損壊類型については、当該データの損壊のデータ処理への悪影響を考慮して動作阻害(イ)を検討することになる。もっとも、2つの類型には、価値判断の基準として別の次元の考慮が入ってくるかもしれず、「損壊」という文言で一つの行為類型として捉えると混乱を招き得るように思われる。コンピュータ・ウィルスの送信が、この類型にあたる場合もあれば、後述する②の類型にあたる場合もあるとされるように(97)、データの消去が、この類型にあたるのか、データの消去命令が不正な指令にあたるのかも判然としないところであり、整理が必要なように思われる。

② ア―2　虚偽の情報又は不正な指令の入力類型

次に、データ入力型の2つの行為類型をみる。ここだけみると(「虚偽の情報」についてはより判例の蓄積がある)電子計算機使用詐欺罪と同じ文言が使われており、かつその解釈も、形式的には同じである。

すなわち、「虚偽の情報」とは、当該システムにおいて予定されている事務処理の目的に照らし、その内容が真実に反する情報のことをいい、「不正な指令」とは当該事務処理の場面において、与えられるべきでない指令のことをいうとされる(98)。

---

(95)　中山研一＝神山敏雄『コンピュータ犯罪等に関する刑法一部改正(注釈)改訂増補版』105頁〔新保佳宏〕(1989)。

(96)　岡田好史「ハッキング・クラッキングに対する刑事規制」現代刑事法57巻35頁、37頁(2004)。

(97)　伊藤ほか・前掲注(81)150頁〔島田聡一郎〕。

最終判断のためには「事務処理の目的」や「事務処理の場面」との関係での比較が不可避であるが、これは、後述の第４目で述べることにする。

本罪における虚偽の情報と不正な指令の関係は、一定の事実情報がデータ化されたものがプログラムに入力され、一定の条件のもとに一定の命令が実行される場合に、真実の事実情報とは異なる意味を持つデータを入力した場合に「虚偽の情報」を与えたと評価され[99]、命令を実行するための条件を充たしていないのに強制的に命令を実行するような指令[100]が「不正な指令」だと評価されている。例えば、化学工場において、電子計算機がある化学反応のために反応器を一定の温度、圧力に保つという制御が行われている場合を考える。このときに、当該反応器の温度、圧力についての事実と異なるデータが「虚偽の情報」であり、停止すべきでない時点での停止命令が「不正な指令」である[101]。

「指令を与え」の解釈としてキーボードからの直接入力や、プログラムに含まれるインストラクションの(予約)実行が含まれるとされる[102]。しかし、まず入力の客体を考えると、こうした手段を用いて虚偽の情報の入力を行うことも考えられよう。また、データ入力は技術発展に応じてセンサ等の様々な新しいインタフェースを介して行われることもあり

---

98 『大コンメンタール刑法 第３版 第12巻』249頁〔鶴田六郎＝河村博〕。

99 DoS攻撃の場合において、データを送っている攻撃者は攻撃対象のコンピュータにアクセスする意思を有していないが、データを送っている時点でアクセスする意思を表明しているのだとすれば、その点において虚偽といい得るという考え方が紹介されている(宇賀ほか編・前掲注69)255頁〔佐伯仁志〕参照)。

100 宇賀ほか編・前掲注69)255頁〔佐伯仁志〕は意味不明なデータを不正な指令に含めるが、同書もその直後にて指摘するように、「その他の方法」に処理不能データ(処理できないが処理を試みる等によりマシンに負荷をかけはするデータ)の入力が挙げられていることを踏まえると、その他の方法にあたる、とするのが通常かもしれない。夏井・前掲注74)208頁-209頁も参照。

101 『大コンメンタール刑法 第３版 第12巻』249頁〔鶴田六郎＝河村博〕。

102 『大コンメンタール刑法 第３版 第12巻』249頁-250頁〔鶴田六郎＝河村博〕。

得、規定はその点を限定しているとも解されない。以上を踏まえると、データ入力の態様は問わない、と解される。

③　ア―3　その他の方法

「その他の方法」が規定されているために動作阻害惹起行為に限定はないともされる(103)。「その他の方法」の例として、電子計算機の電源の切断のほか、温度、湿度といった動作環境の破壊、通信回線の切断、入出力装置等の損壊、処理不能データの入力などがあるとされる(104)。入出力装置や(入力された)処理不能データは電子計算機の一部といい得るので、部分的に既に他の要件でも捕捉し得る点があるようにも思われるが、温度や湿度といった外的な動作環境の変更は「その他の方法」で捕捉するほかない。

もっとも、この要件は、電子計算機に向けられた加害手段であって、当該電子計算機の動作に直接影響を及ぼすものに限定される(105)と解されている。この解釈は電子計算機内に客体としての電磁的記録も存在することを前提としている。すなわち、運搬中の入力データを損壊して事務処理を不能にする行為は、電子計算機の動作自体に「直接の」物理的影響を及ぼさないことを理由に本条の適用外だとされる(106)。ただし、この解釈は、「その他の方法」という文言だけから導かれるのではなく、むしろ第４目で後述する中間結果の解釈で得られたものを実行行為として理解しているのに過ぎないのではないか。そうでないと、「直接」の限界が導かれないように思われる(107)。例えば、オペレータを脅迫して、電子計算機を処理させない場合は、人の意思や行動の自由を害する結果としての業務の妨害しか生じていないから本罪に当たらないと、「その他の方法」の文脈での議論で説明されているが(108)、限定の手がかりは中間結果たる動作阻害の要件にあると考えられる(109)。

---

(103)　山口・前掲注(70)167頁。

(104)　米澤編・前掲注(55)102頁〔横畠裕介〕。

(105)　『大コンメンタール刑法 第３版 第12巻』250頁〔鶴田六郎＝河村博〕、米澤編・前掲注(55)102頁〔横畠裕介〕。

(106)　西田・前掲注(59)50頁。

(107)　中山ほか編著・前掲注(95)107頁〔新保佳宏〕。

第４目　中間結果としての動作阻害(イ)

（1）　一般論

そこで、動作阻害の要件をみる。本罪では、他の業務妨害罪と異なり、中間結果としての動作阻害の現実の発生が要求される[110]。これは電子計算機自体ではなく電子計算機を介して行われる人の業務を保護するものだとされる[111]。もっとも、行為客体には電磁的記録もあるし、また電子計算機を運ぶ業務を本罪が保護するわけではないのだから、この記述のうち「電子計算機を介して」の部分は正確を欠く嫌いがある。電子計算機によって行われるデータ処理の完全性や可用性を直接に保護することによって人の業務を間接的に保護する犯罪だと理解すべきかもしれない。電磁的記録の損壊等によって実現されるイの結果についても、イで問題となっているのが電子計算機の動作である以上、データの損壊それ自体ではなく、損壊によって発生した正しくデータ処理が行われない状態を業務の妨害、あるいはその原因だと評価する判断過程が存在する。

高速のデータ処理によってなされる膨大な情報処理への影響が大きなものになりやすいからこそ、通常の業務妨害罪よりも重い刑での処罰が可能だと解される。その意味で中間結果の要件は、刑の加重を基礎づけているともいえそうであるが、有意な文言解釈が可能だろうか。

中間結果の要件は２つある。

電子計算機に　使用目的に沿うべき動作をさせず、

電子計算機に　使用目的に反する動作をさせて、

---

(108)　『大コンメンタール刑法 第３版 第12巻』250頁〔鶴田六郎＝河村博〕、米澤編・前掲注(55)104頁-105頁〔横畠裕介〕（趣旨がわかりにくいが、オペレータを間接正犯の道具のように捉え得る場合には、電子計算機に対する直接の加害といい得、本罪の成立を認め得るだろう。オペレータ事例においてコンピュータに対する直接の働きかけを肯定できるのはこの場合に限定されるべきだとするものに日本弁護士連合会刑法改正対策委員会『コンピュータ犯罪と現代刑法』136頁〔村井敏邦〕（三省堂、1990））。

(109)　西田・前掲注(59)50頁。

(110)　芝原・前掲注(78)14頁。

(111)　『大コンメンタール刑法 第３版 第12巻』250頁〔鶴田六郎＝河村博〕。

である。

まず、ここでいう「動作」とは電子計算機の機械としての働きをいう(112)。しかし「働き」とは何かが問題である。多くの場合は、電子計算機の物理的位置が変更されるという場合が想定されていたわけではなく、データ処理が念頭に置かれていたといえる。すなわち、電子計算機が所定の機械制御を実行するため、必要とされている情報処理等のために行う出入力、演算等の働き、という具体化である(113)。

次に、「使用目的に沿うべき動作をさせず」と「使用目的に反する動作をさせて」の２つが分けて規定されている。前者は、使用目的に適合する動作をさせないことであり、後者は使用目的と矛盾する動作をさせることをいうが、解釈というよりは語句の言い換えにとどまろう(114)。むしろ、この２要件につき、両者の区別困難性を指摘しつつ、いずれも、結局、使用目的に沿うべき動作をさせないことだと理解すべきだという考えがあり(115)、正当なように思われる。

なお、この要件は「直接」使用目的と乖離する挙動をさせることと理解すべきように思われる。これにより、この要件の当てはめにおいて、オペレータを脅迫する場合について、直接性の要件が欠けることになる。既に「その他の方法」にあたらないと解することも可能であるが(第３目⑵③参照)、「その他の方法」という抽象的な文言の解釈で「直接」と限定するのは恣意性が入らざるを得ず、妥当でないように思われる。

⑵　「使用目的」の解釈

そうすると動作阻害の要件においては「使用目的」の解釈(特定方法)

---

(112)　『大コンメンタール刑法 第３版 第12巻』250頁〔鶴田六郎＝河村博〕。

(113)　『大コンメンタール刑法 第３版 第12巻』250頁〔鶴田六郎＝河村博〕。

(114)　『大コンメンタール刑法 第３版 第12巻』250頁-251頁〔鶴田六郎＝河村博〕。

(115)　西田〔橋爪補訂〕・前掲注(67)145頁、浅田ほか・前掲注(87) 510頁〔森永真綱〕。

大塚・前掲注(73)166頁は、「動作をさせ」ないとは、電子計算機の活動を停止させることだというが、そうではなく、ここでは使用目的に沿う動作をさせないことを意味すると解すべきである。

が重要になってくる。しかし、抽象的な基準しか定まっていない。「使用目的」は、電子計算機を設置してこれを業務遂行のため使用している者が、具体的な業務遂行において当該電子計算機を使用して実現しようとしている目的のことをいうと解されている(116)。電子計算機の機能自体から導かれる抽象的な情報処理目的というのでは足りない(117)。一方で、文字通り使用者の主観的な要素を基準とするのか、それともその主観に基づいてコンピュータに組み込まれた一定の機能を基準とした評価になるのかはなお曖昧である(118)。

基準自体が曖昧なまま、いくつかの解釈例が示されている。

まず、①商用データベースのデータの一部を不正のものに改変する行為は、当該データベース業者の電子計算機の使用目的はその蓄積したデータの検索、提供にあると認められるので、一部のデータを改変して提供させたのみでは、通常、その電子計算機をして使用目的にそうべき動作をさせず、または使用目的にたがう動作をさせたとはいえず、また、データの改変の結果として、データの提供業務の遂行それ自体が困難となるような場合でない限り、業務を妨害したという要件にも当たらない、と解されている(119)。一方で、②情報提供業者のデータベースに大量の虚偽の情報をインプットすることにより、その業者の情報提供を実質的に無意味にする場合には業務妨害罪になる、という解釈も示されていた(120)。

ここで、①と②を合理的に区別できるのだろうか。使用目的をデータの提供とすれば、技術的にはその内容を問わない前提で、データの提供

---

(116) 『大コンメンタール刑法 第３版 第12巻』250頁〔鶴田六郎＝河村博〕。

(117) 芝原・前掲注(78)14頁。

(118) 団藤・前掲注(60)691頁は、業務の過程においてその電子計算機に具体的に設定されたそれをさす、としており、かなり客観面（電子計算機に設定された値）を重視しているように読める。

(119) 米澤編・前掲注(55)105頁〔横畠裕介〕、西田〔橋爪補訂〕・前掲注(67)145頁〔データベースのデータの一部改ざん事例は本罪に当たらない〕。

(120) 第108回衆議院法務委員会議録４号（昭和62年５月22日）34頁〔法務大臣官房参事官米澤慶治発言〕。

機能は維持されており、①も②も使用目的からの乖離はみられないことになる。一方で、データの意味する内容の真実性を問題とする場合、入力したデータの量を問わず、①も②も真実と異なる情報を提供するデータベースを作る行為にほかならないから、使用目的からの乖離が肯定されることになる。①と②の差異は業務妨害を発生させる危険の程度の問題にすぎないとも思われる(121)。つまり、使用目的からの乖離を量的に評価して業務妨害性と結びつける解釈である。しかし、今度は、使用目的からの乖離と業務妨害性が連動することになる。

次に、③天気予報情報を提供するホームページ内の画像をわいせつな画像データに改変する行為における「使用目的」をどのように特定するかが問題となり得る。③のような事例について、大阪地判平成９年10月３日判タ980号285頁で、「使用目的に反する動作」が肯定された。サーバ設置者にとっての使用目的はデータの提供にとどまり、サイト開設者にとっての使用目的が天気予報情報の提供にあるとし、後者の要素から使用目的に反すると評価されたということは可能である。前者の場合は、上記の①の場合であって使用目的違反がないとし、その理由として、サーバコンピュータの管理者としてはホームページの内容の適正さを管理する権能がないことが指摘されている(122)。これは、情報のレイヤーでの議論をしているといえよう。しかし、ここで問題となっているのはデータの不可変更性(完全性)の問題だともいえる。サイバーセキュリティの観点を含め考え、(サーバ管理者にセキュリティ維持の権限や責務があることを踏まえて、)サイト開設者のデータの完全性を維持することもサーバ設置者のサーバの使用目的に入れることもできるかもしれな

---

(121)「ほんの一部の虚偽情報をインプットして虚偽の情報を客にスムーズにというか、円滑にというか、提供していって、結果的には誤っておったわけでございますが、提供自体はなすことができたというような場合は、どうも業務妨害罪そのものの保護法益の考え方、つまり人の業務の遂行の意思決定あるいはその遂行の実現としての行動の自由といいますか、それを妨害したと言えない範囲内にとどまるものも出てくる」(第108回衆議院法務委員会議録４号(昭和62年５月22日)34頁〔法務大臣官房参事官米澤慶治発言〕)。

(122)　斎野・前掲注(69)414頁。さらに渡邊・前掲注(71)、岡田・前掲注(96)38頁。

い(123)。そうすると、ここでいう使用目的もサイト管理者あるいは同人から権限を与えられた者によってアップロードされたデータを提供することになり、それと異なるデータを提供する場合には使用目的に反する動作を認め得るようにも思われる。

さらに、不正アクセス行為等によってデータを無権限で取得する場合は中間結果の要件を充たさず、かつ一般的に、そのような行為によって業務の遂行が外形的に妨げられるとは認められないので、業務妨害の要件にも当たらないと解されている(124)。もっとも、この点も、電子計算機に設置者の使用目的に違う動作をなさしめて業務を妨害したと解されてしまうとも評価されていた(125)。この評価も不可能ではないが、２つの問題提起が可能である。こうした評価は、データを無権限に取得されないというセキュリティの観点を業務の内容に当然に入れ込むことで、無権限に取得されないように一定のセキュリティが機能している状態を使用目的に沿う動作と理解することで可能になる。もっとも、立案担当者はそのような評価をしないが、その理由としては、まず情報セキュリティ内のCIAを棲分け可能な概念だと理解し、本罪で捕捉されるべきなのはCの侵害ではなく、IAの侵害、すなわちデータ処理の無断変更なのだとすべきかもしれない(126)。上記の①、②における検討と同じく、ここでも、本罪の成立を否定する考え方が、動作阻害の要件と業務妨害の要件をいわば連動させて理解していることを指摘できる。

さらに、農林水産省により、広く国民から意見を求めることに資する目的で、サーバコンピュータ上に開設された書き込み用メッセージボードに、掲示板を閲覧した利用者のコンピュータ上で音楽（尊師マーチ）を

---

(123) 本文とは逆に斎野・前掲注(69)416頁は、サーバコンピュータ設置者は、その顧客のホームページの改変行為について、それが行われれば、信用を毀損され顧客を失うなどの事実上の不利益を有しているが、かといって、そのような事実上の不利益の惹起はサーバ管理者の業務妨害につながらない、という方向での議論を行っている。

(124) 米澤編・前掲注(55)105頁〔横畠裕介〕。

(125) 西田・前掲注(59)51頁、中森喜彦『刑法各論 第４版』76頁（有斐閣、2015）、芝原・前掲注(78)15頁。

繰り返し再生せよとの命令を含む制御文字列を書き込んで、当該音楽を繰り返し流れさせた行為について、本件掲示板の設置、運用目的に反するものであると判断した事例がある(127)。掲示板の仕様どおりの動作をしているといえなくもないところ、裁判所は、「本件掲示板の設置、運用目的に反するものであることは明らか」だとしており(128)、この場合も、掲示板の設置目的との乖離それ自体が業務妨害性と連動していると評価し得る。

(3)「使用目的」と「業務妨害」の連動

以上の考察からすると、使用目的は多層的な考慮がなされる要件であって(129)、その意義の特定が難しい。特に、中間結果の要件と業務妨害の要件とがあてはめにおいて連動してしまっており、冗長な要件が規定されたとも考えられ、規定方式としての問題点が浮かび上がる。

この現象が起こる原因には、「業務」との関係で「使用目的」が決まることにある。電子計算機損壊等業務妨害罪は「電子計算機自体を保護しようとするものではなく、あくまでも電子計算機の働きに依拠する業務を保護する」(130)と立法担当者により説明されている。これは、サイ

---

(126) 不正アクセス禁止法上の不正アクセス罪は、アクセス制御機能に対する攻撃を取り締まっており、同機能は、ネットワーク上のデジタルなIDを提供するものであるから、同罪は、ネットワーク上のID保護を担うものだといえ、C(機密性)の保護とは別である(本款第3項参照)。それゆえ、データの無権限取得の事例については不正アクセス罪で規制されることがある、と述べることができるにとどまる(前田雅英編『条解刑法 第4版』726-727頁)。もっとも、そう解しても、不正アクセス罪と電子計算機損壊等業務妨害罪とは保護範囲を異にすることが明らかであって、同様の取り締り(須之内克彦『刑法概説各論 第2版』100頁(成文堂、2014))として整理すべきではない。

(127) 東京地判平成13年5月29日判時1796号108頁。

(128) さらに、裁判所は「掲示板の開設、運用目的に照らして本来与えられるべきでない指令であり、不正なものであることは明らか」だとしており、実質的に業務妨害へつながる行為であれば不正な指令性をも充たす可能性がある。

(129) 芝原・前掲注(78)15頁。

バーのレイヤー、物理レイヤー、社会レイヤーを考えたときに、サイバー、あるいは物理レイヤーではなく、「業務」という社会的なレイヤーを加味しつつ動作阻害の有無を判断することを法律が予定しており、純然たるサイバーのレイヤーで閉じた「サイバーセキュリティ」侵害とは異質の考慮が予定されていることを意味する(131)。こうしたレイヤーをまたぐ考慮は、一定の理由付けをしようにも恣意的になりやすい点があるといわざるを得ない。それぞれのレイヤー間の有意な結びつきを見つけるためには(周辺諸科学の知見も含めた)よりメタ的な視点(132)が必要になり得るところ、本罪の規定や解釈論においてそれが提供されておらず、単に「業務妨害性」に終着する議論がなされているに過ぎない(133)。

それゆえ、動作阻害の要件で、固有の限定が図られているのかには大いに疑問が残る(134)。すなわち、使用目的と乖離した動作は業務の妨害の危険性を有する動作をすることに他ならず、それは業務の妨害との関係で考えれば足り、中間結果の要件の実態は「データ処理の内容の無権限変更がある場合(データ処理の完全性侵害)」なのではないか、と思われる(135)。それは、③の説明において、「使用目的」との関係については

---

(130) 米澤編・前掲注(55)98頁〔横畠裕介〕。

(131) 例えば、DoS攻撃において、ウェブサイトの利用が停滞した場合には動作阻害の要件を充たさず、ウェブサイトの機能が一時的に停止したり、回線がつながらなくなったりした場合にはこの要件を充たす、という説明(宇賀ほか編・前掲注(69)255頁-256頁〔佐伯仁志〕)も、もしかしたら業務妨害に足る動作阻害の程度という観点から一定の閾値を設定することによって結論の相違を見いだしている可能性がある。

(132) 西貝吉晃「情報刑法・序説」太田勝造『AI時代の法学入門』262頁以下(弘文堂、2020)における架橋論理の使い方参照。

(133) 芝原・前掲注(78)15頁。前掲注(128)も参照。

(134) 本罪を危険犯と解する限り、第二・第三の要件間に実際上どの程度の違いが生じるのかが明確でない、とする指摘に中森・前掲注(125)76頁。

(135) 夏井高人「サイバー犯罪の研究(一)」法律論叢85巻1号197頁、229頁注25)(2012)も、電子計算機損壊等業務妨害罪の規定のうち、行為態様の「虚偽」や「不正」を「無権限」と理解して、結局、「正しくは、「無権限で情報または命令を」とするのが正しく、そのように法改正すべき」だとする。

触れずに、業務妨害性のみを議論して業務妨害罪の成立を認めようとする議論がなされていることからも示唆される。このように理解しても、コンピュータを用いたデータ処理によって初めて可能になった膨大な情報処理が阻害される以上、対人的な業務妨害罪よりも重い法定刑を基礎づけることができると考える。

もっとも、この理解は、中間結果をデータ処理の無権限変更だと理解してサイバーのレイヤーのみの問題に入れ込む議論であって中間結果の要件を実質的に簡素化する議論でもあるから、やや立法論にもよっている。そのため、他国の規定や解釈も見つつ、検討していきたい。

第５項　小括

CPSの保護を考える際にも起点をサイバー攻撃だと考える限りにおいては、上記で紹介したサイバー犯罪対策立法の取り扱い方法が重要になってくる。つまり、①(サイバー)⇒②(フィジカル)の過程、あるいは①⇒②⇒③(社会)の全過程に着目しているのがここで議論したいサイバー・フィジカル・セキュリティに関する犯罪類型である。いずれの場合も、重大な損害が生じ得るように思われるところ、上記で紹介した電子計算機損壊等業務妨害罪の懲役刑の長期が５年であり、サイバー・「フィジカル」・セキュリティの保護を考える上で十分なのか、疑問があり得る。

また、第４項第２目⑵でみたとおり、サイバー・フィジカル・セキュリティの保護を図る上では、後述するように、公共危険犯との関係が極めて重要になりそうである。電子計算機損壊等業務妨害行為によって発生する結果に公共危険犯の結果と同等のものがある場合には、加重規定の創設等を考えるべきかもしれない。

第４節　現行のサイバー犯罪対策立法の限界点

以上の考察からすると、フィジカル面での損害を十分に意識しないで作られたと評価し得るサイバー犯罪対策立法をそのまま用いるには限界がありそうである。むしろ、フィジカル面がどのように保護されているかも考える必要がある。物に対する保護であれば刑法でも建造物損壊罪や器物損壊罪により、場合によっては放火罪等によっても保護がなされている。鉄道や艦船の往来に関しては、刑法上の往来危険罪で保護されて

いる。放火罪や刑法上の往来危険罪の法定刑は類型的に重くなっている。

もっとも、これらの犯罪類型でサイバー攻撃の激化に対応できるか否かが問題となる。なぜなら、サイバー・フィジカル・セキュリティの保護が議論され始めたのは最近のことであり、フィジカル面での保護を行おうとする立法は、サイバー攻撃に対する対策ではなく、物理的攻撃を想定されてなされてきていたといえるからである。また、極めて重要なインフラである航空インフラについて特別法上の罰則が存在するように、形式的意義の刑法のみではフィジカル面での保護を考えるのに十分ではない。CPSが様々な目的で用いられることが予定されていることを踏まえると、特別法上の罰則を、CPSの利用目的に応じて整備することが今後の課題となってくる。

第４章　我が国におけるフィジカル面の保護立法

そこで、サイバー攻撃にさらされたときに甚大な被害が生じうる客体のフィジカル面を我が国の立法がどのように保護してきたか、ということを検討する。サイバー犯罪対策規定は(インフラ等の)客体の種類を問わずに処罰可能であるのに対し、フィジカル面の直接の保護を行う規定の場合、それぞれの客体の特徴に応じた法規制を検討する必要がある。

本章では、保護の重要度が高いと思われる交通インフラ及び電気・ガス・水道インフラ[136]について検討したい。

第１節　交通インフラの保護

交通の安全は、社会生活、経済・産業の発展・成長にとって重要な意味を持ち、交通機関の大型化及び高速化と相まって不特定又は多数人の生命・身体及び財産に対する危険と直結するので、その維持を図るために一面において公共危険犯をもって臨む必要がある[137]。

---

(136)　熊谷ほか・前掲注(34)1518頁も、鉄道、電力、水道、ガスを最初に例示して分析を進めている。

(137)　団藤重光編『注釈刑法(3) 各則(1)』206頁〔高田卓爾〕(有斐閣、1965)。

第１款　鉄道の安全

鉄道の安全は基本的には刑法の往来危険罪(125条１項、２年以上の有期懲役)で保護される。往来妨害罪(124条)は鉄道交通を保護しない[138]。もっとも、各種自動設備を搭載したいわばハイテク電車である新幹線については、新幹線を特別に保護する立法(新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法(以下「新幹線特例法」という))により、その安全が特に保護されている。

第１項　往来危険罪(鉄道)

往来危険罪は、往来の安全を保護し、かつ「その他の方法」として、行為態様を限定しない[139]。本罪は、(実害発生の立証までは不要であるが、)往来の安全を害すべきおそれのある状態の発生を要件とする具体的危険犯だと解されている[140]。もっとも、往来危険の発生というためには、事故等の実害発生の必然性、切迫性は不要で、その可能性で足りるとされ、同要件の評価は緩やかだと評されている[141]。

それでも、例えば、①信号操作を放置して電車を停止させた事例[142]、②列車の自動連結器を解錠して列車を分離し、分離した部分の軌条上に立て札を投げ入れ、分離した状態で貨物列車が発車したが、制動がか

---

⑬⑧　山口・前掲注⑦⓪404頁。往来妨害罪にいう「陸路」とは道路のことであって、「橋」についても鉄道自体またはその構成物(例えば、電車・列車の通る鉄橋等)といった専ら鉄道交通に供されているものを含まない(伊東研祐『現代社会と刑法各論 第２版』327頁(成文堂、2004)、浅田ほか・前掲注⑧⑦289頁〔照沼亮介〕)。鉄道も陸路(道路)といえなくもないが、刑法125条との関係からいって除外される、という説明もあるが(団藤編・前掲注⑬⑦207頁〔高田卓爾〕)、そういえてしまうのであれば、より軽い往来妨害罪について特に限定するように解釈すべき理由の説明が必要になると思われる。

⑬⑨　大塚仁＝河上和雄＝中山善房＝古田佑紀編『大コンメンタール 第３版 第７巻』212-213頁〔渡邉一弘〕(青林書院、2014)(以下『大コンメンタール 第３版 第７巻』として引用)。

⑭⓪　『大コンメンタール 第３版 第７巻』220-221頁〔渡邉一弘〕。

⑭①　平野龍一『刑法 総論Ⅰ』121頁(有斐閣、1972)、山口厚『危険犯の研究』11頁、143頁以下(有斐閣、1982)。

⑭②　最判昭和35年２月18日刑集14巻２号138頁。

かって約５メートル進行して停車した事例[143]で往来危険の発生が否定され、さらに、③列車のポイントを反位に切り替えた行為につき、一般的には往来危険を生ずる行為だが、列車は絶対運行しないとの確信があった事例において故意が否定された[144]。

列車が進行を始めた直後でも危険発生がないとされた②の事例、及び列車が運行しないことを往来危険の消極判断の基礎にし得ると思われる③の事例[145]によれば、システムへの侵入（ハッキング）により電車の移動や停止を「可能にした」だけでは往来危険の発生を肯定し難い。往来危険罪には未遂犯処罰規定があるが、それが積極的に活用されているようには思われない。

そうすると、コンピュータでコントロールされている交通機関のコンピュータをハッキングして制御用データを改変して電車を停止等させた場合に往来危険の未遂も成立しない可能性がある[146]。サイバー攻撃に基づくシステムへの侵入それ自体に対して具体的危険犯である往来危険罪を実効的に使うことが難しい場合があり得そうである[147]。

第２項　新幹線特例法

そこで、通常の鉄道よりも高速度で運行することが前提となる新幹線の運行の安全を特に保護する立法をみてみる。新幹線特例法は、新幹線がその主たる区間を200km/h以上の高速度で走行できることに鑑みて（法１条）、特に運行の安全を罰則で担保しようとしている。規定も述べるように、本法は鉄道営業法の特別法でもある。鉄道営業法上の罰則についても、高速度交通機関の持つ社会的使命と事故による結果の重大性

143　仙台高判昭和31年５月９日仙台高検速報昭和31年47号。

144　広島高判松江支判昭和29年12月13日高刑集７巻12号1747頁。

145　山口・前掲注(141)145−146頁は、犯罪の客観面の判断において限定がかけられた可能性を指摘する。

146　新保佳宏「業務妨害罪をめぐる諸問題」犯罪と刑罰３号97頁、102頁（1987）は本文のような場合に往来危険罪の成否を考えれば足りるとしていたが、そうでもないように思われる。

147　この点については既に検討した。西貝吉晃「コネクティッドカーシステムに対するサイバー攻撃と犯罪」法時1136号48頁、49頁（2018）。

を考慮すべきだと思われるものの(148)、それを考慮すると、本罪自体の法定刑の低さに問題があり得る。この点は脚注(149)を参照されたい。ここでは新幹線特例法の検討を行う。

新幹線及びその周辺のシステムでは、ヒトによる肉眼での確認に基づ

---

(148)　平野龍一＝佐々木史朗＝藤永幸治編『注解特別刑法２　交通編(2)』鉄道営業法23頁〔原田國男〕(青林書院、1983)。

(149)　鉄道営業法25条が、鉄道係員による職務上の義務違反等による「旅客若ハ公衆ニ危害ヲ醸スノ虞アル所為」を処罰する。同条は過失犯も処罰する(大判大正７年６月11日刑録24輯838頁、平野ほか編・前掲注(148)鉄道営業法15頁〔原田國男〕、黒川英夫「鉄道犯罪に就いて」司法研究第５輯報告書集７号１頁、25頁(1927))。例えば、本条に該当する場合として客車の横戸を開いたまま運転する行為が挙げられていた(喜安健次郎『改正鉄道営業法』307頁(鉄道新聞社、1930)、馬屋原成男編著『鉄道犯罪の解説』23頁(盛文社、1948))。もっとも、実際上は、業務上過失致死傷罪や業務上過失往来危険罪を検討すべき場合の方が多いゆえに、本条それ自体の意義は大きくない。また、往来危険罪が成立する場合は同罪の成立が優先する(法条競合、前掲原田23頁。業務上過失致死傷罪とも法条競合になるとするものに前掲馬屋原23頁)。

「危害ヲ醸スノ虞」に関連し、本罪の罪質について抽象的危険犯か、具体的危険犯か、争いがある。抽象的危険犯説は、旅客・公衆に現実に危害が及んだことや、危害が及ぶ現実的危険が発生したことは不要だとする(安西温『改訂 特別刑法１』299頁(警察時報社、1990)、前掲馬屋原23頁)。抽象的危険犯説には、具体的危険犯である往来危険罪との間の棲分けをより明確にし得る機能がある。

もっとも、抽象的危険犯だとする伊藤榮樹＝小野慶二＝荘子邦雄『注釈特別刑法 第６巻II 交通法・通信法編 新版』８頁〔伊藤榮樹(河上和雄補正)〕(立花書房、1994)は職務上の義務違背があったが旅客・公衆の生命身体に危害をもたらすおそれを生じなかった場合には本罪が成立しないとしているので実質的に具体的危険犯説である(前掲原田20頁以下が、この要件を行為に内在するものとしてみるか、結果とみるかについて本質的でないと指摘するのは伊藤検事の記述に由来しているかもしれない)。そして、裁判例(東京高判昭和38年12月11日判時385号71頁、広島高判平成19年５月29日判タ1252号343頁)も具体的危険犯説をとる(さらに武藤眞朗「判批」高橋則夫＝松原芳博編『判例特別刑法』94頁以下(日本評論社、2012))。

く制御ではなく(150)、各種自動設備(151)が利用されており、列車運行の効率化及び安全の保持を達成しようとしている。これらの設備はフェイル・セーフ方式(誤作動等が発生した場合に安全な状態に移行する方式)を採用しており、不具合が発生しても直ちに危険が生じることはないように作動するようになっている。もっとも、例えば多重に防御されているシステムだからといって、無権限での操作を許すと、システムの保護を十分に達成できない。サイバー・セキュリティと刑法的規制の関係について、既に技術的な防御措置がなされているからといって、刑法的な規制が不要になるわけではない。この理解は、サイバー・セキュリティの維持だけでなく、サイバー・フィジカル・セキュリティの維持の側面でも成立すると考えられる(152)。それゆえ、フェイル・セーフ方式と刑法的保護の両側面から不適切な行為を抑止する必要がある(153)。

新幹線特例法による無権限操作等の防止態様をみていく。

第１目　新幹線特例法２条１項の罪

各種自動設備を損壊し、その他これらの設備の機能を損なう行為をした者(可用性の低下または喪失)が５年以下の懲役または５万円以下の罰

本罪を具体的危険犯と解する場合、往来危険罪との関係での守備範囲の棲分けが問題になり得る。この点、本罪の過失犯の設例として台車に亀裂の入った車両で走行し続ける場合が業務上過失往来危険罪の手前のものとして挙げられるが(和田俊憲「注釈鉄道営業法罰則」慶應法学40巻229頁、235頁(2018))、故意によるハッキングの問題を考えるにあたっては本罪の検討を中心に置く必要は大きくないと考える。

(150)　伊藤・前掲注(30)12頁-13頁。

(151)　自動列車制御設備(ATC)、列車集中制御設備(CTC)、自動針路設定設備、自動列車検知設備、非常列車防護設備。以上、新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法施行規則参照。

(152)　伊藤・前掲注(30)13頁は、各種設備を設けたり、運転士の教育訓練の徹底をはかったり、また、施設面において全線にわたって立体交差として踏切事故をなくしたり、線路内への立入り、物件の落下を防ぐため、必要な箇所に防護柵を設置したりしているが、さらに新幹線特例法上の刑罰が必要だと指摘する。

(153)　伊藤・前掲注(30)17頁、井上・前掲注(30)53頁。

金に処せられる（新幹線特例法２条１項）。本罪は刑法125条１項の往来危険罪及び器物損壊罪(154)の特則であって、これらの罪とは法条競合になる(155)。重い法定刑を有することを踏まえると、本罪は、上記自動設備を損壊等から保護することによって、新幹線鉄道の運行の安全を確保しようとする、危険犯だと解される。そして、問題となっている行為自体が列車の運行上極めて危険であることを理由に事故発生の危険を要件としない抽象的危険犯だと解されており(156)、具体的危険の発生は不要である(157)。損壊したものの、設備がフェイル・セーフの方向に作動して具体的危険が発生しなかった場合にも本罪は成立する(158)。事故発生のおそれの認識は本罪の故意の内容ではない(159)。事故発生のおそれの認識があると往来危険罪ないしその未遂罪が成立する可能性があり、その場合には、往来危険罪のみが成立する(160)（法条競合の吸収関係）。

行為態様としての「損壊」は、①客体たる設備それじたいの全部または一部を物理的・有形的に変更して（ハンマーによる破壊や部品の抜き取り等）、②その全部または一部を害することである(161)。器物損壊罪における損壊は物理的・有形的な変更以外の行為態様も含むから、これより

---

(154)　運行の安全を保護するために、財産的価値を保護する器物損壊罪で器物損壊罪で臨むのは妥当でない（井上・前掲注(30)50頁）。

(155)　安西・前掲注(149)290頁、292頁。

(156)　安西・前掲注(149)290頁、井上・前掲注(30)50頁。

(157)　伊藤・前掲注(30)19頁。

(158)　伊藤・前掲注(30)19頁。

(159)　平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法22頁〔平本喜禄〕。

(160)　平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法22頁〔平本喜禄〕、伊藤・前掲注(30)19頁−20頁。なお、具体的危険の発生の認識がない場合に往来危険が発生した場合には過失往来危険罪が成立し得、本罪と観念的競合になるという指摘がある（井上・前掲注(30)57頁）。

(161)　安西・前掲注(149)291頁−292頁、平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法20頁〔平本喜禄〕、伊藤・前掲注(30)18頁。

もよりも狭い(162)。さらに、①だけ充たし、②を充たさない場合には、その設備本来の機能を害するおそれがある場合にのみ、３項の「損傷」にあたるにすぎない(163)。

行為態様としての「その他これらの設備の機能をそこなう行為」は、「損壊」以外の行為であって(有形的変更を伴わない場合であって(164))設備本来の機能を害する一切の行為である(165)。電磁波を受ける機能を有するATC装置等の地上子を金属片で覆って電磁波を全く受信できないかまたは正確に受信できないようにする行為がこれにあたる(166)。

損壊は器物損壊罪のそれよりも狭く解されているが、上記の通り、機能障害行為も別途捕捉されており、これにより、通電を停止させて機械の運転を停止させて、一時的にその効用を害する場合等を、損壊で無理に拾うことなく、機能障害で拾うことができるとして、文理に忠実に妥当な捕捉範囲を保てるという指摘がある(167)が、妥当だと考える。

さらに、法２条１項の罪の未遂的行為(168)が５万円以下の罰金に処せられる(新幹線特例法２条３項)。ただし、行為態様が「第一項の設備を損傷し、その他同項の設備の機能をそこなうおそれのある行為」として具体的に規定されている。立法動機には、新幹線の運行保安設備の重要性を踏まえ、その行為自体によって設備の機能が損なわれるところまで

---

(162) 平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法20頁〔平本喜禄〕。

(163) 平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法21頁、26頁〔平本喜禄〕。

(164) 井上・前掲注(30)57頁。

(165) 平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法20頁〔平本喜禄〕、伊藤・前掲注(30)18頁。

(166) 平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法20頁〔平本喜禄〕。

(167) 平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法20頁−21頁〔平本喜禄〕。さらに、井上・前掲注(30)55頁−56頁の指摘も参照。

(168) 平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法25頁〔平本喜禄〕、伊藤・前掲注(30)22頁。

いかなくても、他の条件が加わってその機能が損なわれる危険がある場合にはなお当罰的だという考慮がある(169)。ここで、「損傷」とは、物理的有形的変更による場合である(170)。ケーブルの切断は損壊だが、その被覆を取り除いて雨水による腐蝕の危険を作り出す場合が損傷の例として(171)、地上子の上に小さな金属片を置く行為がその他の機能をそこなうおそれのある行為の例だとされる(172)。

第２目　新幹線特例法２条２項の罪(みだりに操作罪)

次に、法２条２項にみだりに操作罪が規定されている。本罪も１項と同様、抽象的危険犯だと解されており、客体をみだりに操作するだけで成立する(173)。みだりに操作することにより、ただちに新幹線の全線の列車運行に大きな影響を与えることとなると予想されることが罪質を決定づけている(174)。故意犯なので単なる操作の誤りは処罰されない(175)。

「操作」とは「所携の設備を、その本来の使用方法に従って作動させること」だと解されている(176)。そして「みだりに」とは、正当な理由がないことを意味するとされ、これには、当該設備を操作する資格・権限のない者が操作する場合、及びその資格・権限のある者が所定の操作指示によらずに、またはその設備の本来の使用目的に従わない方法で操作する場合が含まれる(177)。外部者、内部者を問わず処罰することが可能な規定だといえる。

---

(169)　伊藤・前掲注(30)22頁。

(170)　平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法21頁、26頁〔平本喜禄〕、伊藤・前掲注(30)22頁〔他の条件と相まって物の効用を害する危険性がある場合だという〕。

(171)　平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法21頁、26頁〔平本喜禄〕。

(172)　伊藤・前掲注(30)21頁−22頁、井上・前掲注(30)59頁。

(173)　安西・前掲注(149)293頁、井上・前掲注(30)53頁。

(174)　伊藤・前掲注(30)20頁。

(175)　伊藤・前掲注(30)21頁。

(176)　平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法24頁〔平本喜禄〕、井上・前掲注(30)57頁、安西・前掲注(149)292頁。

「みだりに」を無権限と、「操作」をシステムの利用の開始と捉え直すことも可能だと思われる。そうすると、サイバー攻撃との関係では、みだりに操作とは、自動的に一定のデータ処理を行うシステムに侵入して無権限に利用を開始することだともいえる。さらなる検討が必要になり得るが、利用の開始とは、一定の重要なシステム上のプログラムを起動することや当該プログラムにコマンドを送信することだとも考えられ、また、無権限についても外部者・内部者を問わずに適用可能な概念であるから、特定の重要なシステムの無権限利用罪として、みだりに操作罪を捉えることができそうである。

もっとも、サイバー攻撃に限って処罰したい場合には、現行の不正アクセス罪とは別の、特定のコンピュータの利用を無権限(内部者による権限の超過を含む)で開始した場合に処罰可能とする特別な不正アクセス罪の新設を考えてもよいかもしれない。

また、１項、２項の罪の双方にいえるが、往来危険罪のところで述べたところと異なり、(危険擬制説的な)抽象的危険犯を利用することで、可用性の確保が絶対的に重要な設備に対するサイバー攻撃それ自体を類型的に捕捉することができそうである。

第２款　船舶の安全

鉄道は軌道上を走行するものであるが船舶はそうでない等、性質上の相違は存在するものの、我が国の現行刑法は、艦船の往来の安全を往来危険罪や往来妨害罪等により保護している。船舶の安全は刑法上の往来危険罪の規定(125条２項)、及びより軽い往来妨害罪の規定(124条、２年以下の懲役又は20万円以下の罰金)で保護される。

第１項　(水路等への)往来妨害罪及び往来危険罪

水路についての往来妨害罪は、水路(艦船等の航行の用に供され、公衆の往来の用に供される河川・運河・港口等)に対する往来妨害惹起行為の全てを処罰するわけではなく、物理的に損壊または閉塞する場合のみを処

---

(177)　平野ほか編・前掲注(148)新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法23頁〔平本喜禄〕、安西・前掲注(149)292頁−293頁、伊藤・前掲注(30)21頁、井上・前掲注(30)57頁−58頁。

罰しており、行為態様が限定的である。

ここで、ハッキングを直接処罰するために、ハッキングによる制御乗っ取りや暴走可能化行為自体が権限ある者による制御を妨害していることは確かであるとして、往来妨害罪の規定を拡張的に解するという解決もあり得るかもしれない。例えば、刑法改正仮案は、現行法中の往来妨害罪の規定中の行為態様を「其ノ他ノ方法ヲ以テ」を付して拡張しようとしていた(仮案275条[178])。こうすることで、ハッキングによる往来妨害も捕捉されるかもしれないが、ハッキング以外のあらゆる行為態様まで捕捉することになり、それでよいかが問題となる。

また、本罪は、円滑な通行を保護しようとするものであって、相当な時間にわたっての行為(損壊・閉塞)の効果の継続を要求する[179]。ハッキングや不正な指令の送信による権限ある者による制御の妨害と、事象として一対一対応している保障もない。

第２項　水上交通の安全を図る特別法規

後述の本節第３款第３項で述べるハイジャックに対応するシージャックを防止する直罰規定は置かれなかった[180]。その代わり、やや細かな諸規定が置かれている。法体系的にみると、船舶それ自体の物的安全(船舶安全法)や、船舶の運航を担当する職員の技能的保障に基づく安全(船舶職員及び小型船舶操縦者法)といった観点から、航行の安全を保障し

---

(178)　現行刑法においても、この仮案に倣って行為態様を拡張的に捉えようとして、例えば、詐欺の標識の設置行為を往来妨害罪の行為態様に含むとするものもあったが(牧野英一『刑法各論(上巻)』105頁(有斐閣、1950))、刑法125条のような「その他の方法」という規定がない以上、厳格解釈が要求される刑法においては、それは無理な解釈であろう。

(179)　『大コンメンタール 第３版 第７巻』202頁〔渡邉一弘〕。

(180)　船舶の機能・形状が千差万別であって一般的な規制になじむかわからない、という懸念が示されていた(大村行雄「航空機の強取等の処罰に関する法律について」41巻７号23頁、28頁(1970))。もっとも、刑法改正草案第14章においては、公共の法益を保護する罪として、船舶及び航空機の強奪及び運航支配の罪が置かれている(法制審議会刑事法特別部会『改正刑法草案附同説明書』197頁-199頁(法曹会、1972)。さらに平場安治＝平野龍一編『刑法改正の研究２　各則』239頁-242頁〔西原春夫〕(東京大学出版会、1973))。

ようとしているといえそうではある。また、海上衝突予防法が、罰則を使わずに、海上における衝突事故を防ぐための基準を提供している。海上交通安全法26条１項や35条は、一定の場合に「船舶交通の危険」の発生を防止するための措置を海上保安庁長官がとることを認めており、同法47条２号がこれらに関する処分に違反する行為を処罰している（３月以下の懲役又は30万円以下の罰金）。

第３項　内部者犯行への対応

水上交通に関し、内部者犯行への対応策として例えば職権濫用罪を挙げることが出来る。例えば、水上交通に関し、船員法122条が船長（及び船長に代わってその職務を行う者（船員法134条、以下「船長等」という））による船内にある者に対する職権濫用罪を規定する。しかし、サイバー攻撃は対人的攻撃であるとは限らないし、船舶交通の危険は、第三者の行為を介さなくても可能だと考えられるから、職権濫用罪に頼るべきではない。

第４項　小括

以上の法規制は船舶がサイバー攻撃のリスクに常に晒されている時代が来た場合には、この規定では、場合が限定されすぎているとも思われる。一方で、水上交通の特徴を踏まえた規制であり、部分的に行政的措置も介在しているところをみると、サイバー攻撃の激化だけを理由にこれらの特別法規を抜本的に改正すべきというには慎重になるべきかもしれない。

第３款　航空の安全

第１項　総説

条約の要請もあって、1980年代のコンピュータ犯罪対策立法よりも前に、航空の安全に対する攻撃に対しては、航空危険罪（航空の危険を生じさせる行為等の処罰に関する法律１条の罪[181]（以下「航空危険行為等処罰法」））、運航支配罪（航空機の強取等の処罰に関する法律１条、予備・未遂が可罰的）、運航阻害罪（航空機の強取等の処罰に関する法律１条、予備・未遂は不可罰）といった処罰立法が整備されている。これらの犯罪類型は刑法上の犯罪類型と類似しているが、異なる部分もある。サイバー攻撃の問題とは別に、刑法上の往来危険罪等に統合しようという立法的な動き

もあったが(改正刑法草案198条等)、実現していない。航空危険罪から順にみていく。

第２項　航空危険罪

第１目　罪質等

航空危険罪は既に説明した往来危険罪(刑法125条)の航空版である[182]。刑法に規定されていないのは刑法が明治40年に立法されたという時代的なものである。サイバー攻撃の問題を抜きにしても、立法論としては重要インフラたる航空の安全も刑法上の往来危険罪に取り組むことも検討され得る[183]。

航空危険行為等処罰法１条は「飛行場の設備若しくは航空保安施設を損壊し、又はその他の方法で航空の危険を生じさせた者は、３年以上の有期懲役に処する」と規定する。航空機の航行の安全を保護することによって不特定多数人の生命を保護している。同法２条以下においても、極めて重大な犯罪として、墜落罪(無期又は３年以上の懲役)や墜落等致死罪等(死刑又は無期若しくは７年以上の懲役)が規定されている。これらの罪においては、未遂犯が可罰的であるが(同法５条)、予備罪は可罰的でない。

---

[181] その前身は航空法138条にあったが、航空法内での改正は、モントリオール条約の批准のために早期の立法が必要であること、本法で使われる一定の概念についての定義が航空法にはないことや国外犯処罰規定が航空法になじみにくいこと等を理由に断念された(第72回国会衆議院交通安全対策特別委員会会議録第11号(昭和49年４月３日)５頁〔運輸省航空局長寺井久美政府委員発言〕)。

[182] 安西・前掲注[149]258頁、山口真弘『航空法規解説 全訂版』498頁(航空振興財団、1993)。【旧航空法上の航空危険罪】住田俊一『航空法精説』303頁-304頁(日本航空整備協会、1969)は往来危険罪のアナロジーで航空危険罪を議論する。

[183] 『大コンメンタール 第３版 第７巻』211頁〔渡邉一弘〕、吉永祐介「いわゆるモントリオール条約と航空危険行為等処罰法」警察学論集27巻８号192頁、209頁(1974)。なお、刑法改正草案198条は、輸送機関の発達に伴い(平場＝平野編・前掲注)[180]233頁〔西原春夫〕、汽車・船舶・航空機の交通危険罪を有している(法制審議会刑事法特別部会・前掲注[180]195頁-197頁)。

本罪と刑法上の暴行、脅迫、器物損壊、建造物損壊とは法条競合となって本罪のみが成立し、本罪と業務妨害罪とは観念的競合になると解されている(184)。

要件群をまとめると次のようになる。

飛行場の設備 航空保安施設 その他の方法で	を損壊し	航空の危険を生じさせた

第２目　行為態様の無限定性

同法１条の航空危険罪の行為態様として掲げられる「その他の方法」は、航空の危険という結果を生ぜしめるに足りる一切の作為・不作為と解されている(185)。立法時には、「その他の方法」は損壊に準ずるものと理解されていたが(186)（行為の拡張アプローチ）、上記の定義を踏まえ、「その他の」という文言の用例に従ってみれば、飛行場の設備の損壊等というのは例示であって、結局のところ同罪の行為態様は、実際上、無限定なものになっていると評価できる（結果からの演繹アプローチ）。本罪で防止の目的となる事故が多数人の死傷を伴い得る重大なものであることに照らせば、行為態様の種類を限定しない解釈には理由があると思われる。

「その他の方法」には、航空保安施設への送電の停止、航空保安無線の施設の効用を阻害するような電波の発射、時限爆弾を航空機にセットしている等という虚偽通報が含まれると解されていたから(187)、サイバー攻撃によって飛行場の設備の機能不全等を発生させ、結果として航空の危険が生じた場合にも「その他の方法」にあたると解するに妨げはなく、本罪で処罰され得る。

---

(184)　吉永・前掲注(183)211頁-212頁。

(185)　吉永・前掲注(183)211頁、安西・前掲注(149)259頁。
不作為の例として「整備員が航空機のタイヤの異常に気付きながら故意にそのままにしておいた場合」が挙げられている。

(186)　第72回衆議院交通安全対策特別委員会議録13号（昭和49年４月11日）17頁〔法務省刑事局長安原美穂発言〕。

上記の通り、行為態様の無限定性が強調されるべきところではあるが、規定解釈は次のようになっている。その他の方法以外は「損壊」のみが捕捉される。ここでいう「損壊」の概念は、客体たる物それ自体を物理的、有形的に変更することによって、その物本来の機能の全部又は一部を失わせることをいう(188)。

「飛行場の設備」とは、飛行場の機能を果たすために必要な一切の施設、設備で、飛行場の敷地内に存するいのをいい、例えば、滑走路、着陸帯、誘導路、エプロン、飛行場標識施設、給油施設、無線施設、ターミナル・ビル等がこれにあたる(189)。「航空保安施設」の定義は航空法２条５項(190)にある。

第３目　具体的危険犯

航空危険罪は具体的危険犯である(191)。それゆえに、航空機の衝突・

---

(187)　吉永・前掲注(183)211頁、第72回衆議院交通安全対策特別委員会議録13号（昭和49年４月11日）17頁〔法務省刑事局長安原美穂発言〕。そもそも、簡単に沿革をたどってみれば、戦前の、多数人の共同作業によって信号を行っていた時代における航空危険罪（航空法49条）は「詐欺ノ信號ヲ為シ又ハ其ノ他ノ方法ヲ以テ航空ノ危険ヲ生セシメタル者ハ二年以上ノ有期懲役ニ処ス」と規定していたのであり、そもそも、損壊類型ではなく、判断を誤らせる点が重視されていたことがわかる（長尾猛夫「航空に関する犯罪」司法研究第15輯１号69頁−71頁（1932）参照）。 CPSのセキュリティの観点からも、機器の誤作動を惹起させることは、複雑に構成されたCPSに対する重大な侵害であることは明らかであって、その他の方法にCPSへのハッキングが入ると解することは、沿革からしても自然な考え方であると思われる。

(188)　吉永・前掲注(183)211頁、安西・前掲注(149)259頁。

(189)　吉永・前掲注(183)211頁。

(190)　航空保安施設は「電波、灯光、色彩又は形象により航空機の航行を援助するための施設で、国土交通省令で定めるもの」のことをいい（航空法２条５項）、この規定を受けた航空法施行規則１条は航空保安施設として、航空保安無線施設（電波により航空機の航行を援助するための施設）、航空灯火（灯光により航空機の航行を援助するための施設）、昼間障害標識（昼間において航行する航空機に対し、色彩又は形象により航行の障害となる物件の存在を認識させるための施設）の３つを挙げる。

(191)　吉永・前掲注(183)211頁、安西・前掲注(149)259頁。

墜落・転覆・破壊・火災等の事故発生の可能性がある状態（航空の危険＝航空の往来の危険[192]）を発生させることが必要である[193]。もっとも、現実の事故発生や、事故発生の高度な蓋然性は不要である[194]。これも故意の内容になると解され、すなわち、故意としては航空機の衝突・墜落等の事故を惹起するおそれについての未必的な認識が要求される[195]。数多くのインフラに無差別にサイバー攻撃を加えるような場合に、その中にたまたま飛行場の設備等が含まれていたものの、そのことについて、犯人としては未必的な認識さえなかった、という場合には、本罪の成立を肯定できない。

第３項　運航支配罪及び運航阻害罪

航空危険罪とは別に航空機自体の制御に対する攻撃、いわゆるハイジャックに対する抑止を強化する趣旨から、航空機の強取等の処罰に関する法律が、強盗罪的な運航支配罪（法１条〔無期又は７年以上の懲役〕）と業務妨害罪的な運航阻害罪（法４条〔１年以上10年以下の懲役〕）の２つの犯罪類型を有し、前者にのみ致死罪を付加している。これらの犯罪類型は運航に関する制御の乗っ取り又は攪乱行為に利用し得ると思われ、また、規定ぶりやそこから得られる解釈も、サイバー攻撃に対する方策として参考になり得る。他方、これらの規定は1980年代のコンピュータ犯罪対策立法施行前に作られたものなので、サイバー犯罪との関係での規定の整備の必要性も含め、以下検討する。

第１目　航空機の運航支配罪

まず、運航支配罪は、強盗的態様でハイジャックが行われることを踏まえつつ、強盗罪を模しながらも、機長により占有・支配されている航行中の航空機の乗っ取り行為（強取、運航支配）を強盗罪よりもより広く、かつより重く処罰する。ハイジャックにおいては、航行中の航空機の密室性に基づいて比較的容易に強盗的行為が可能であること、同行為は財

---

(192)　【旧航空法上の航空危険罪】住田・前掲注(182)304頁。

(193)　吉永・前掲注(183)211頁、安西・前掲注(149)259頁。山口真弘・前掲注(182)498頁−499頁は刑法上の往来危険罪の判例を援用する。

(194)　安西・前掲注(149)259頁。

(195)　安西・前掲注(149)259頁。

産上の甚大な被害、航空業務の著しい妨害、不特定多数の乗客に対する監禁や恐怖付与等をもたらすから(196)、これらを踏まえれば、不法領得の意思がなくとも、強盗よりも重く処罰することが正当化されるだろう。例えば、強盗罪は財産犯であって不法領得の意思(少なくとも第三者への加害目的だけでは認められないような、その物を自分のために利用する意思)が必要だと解されているが、同意思は運航支配の要件ではない。第三者加害目的しかない場合でも運航支配といえるし、財産上の利益を得る意思がない場合で乗客が目的地に到着するのを阻止する目的で出発地に引き返させる場合も運航支配である(197)。運航支配を構成要件的行為に含む本罪は、結局のところ領得罪とはいえず、放火罪のように、財産保護の要素を併有しつつも、不特定多数人の生命への抽象的危険犯と理解される犯罪に近い(198)。

強取も運航支配も、運航権限を奪取し、自己の意のままに運航させることをいう(199)。強取については解釈上の争いがあり得るが、共に権限奪取に基づく運航が継続する限り犯罪が終了しないと解されている(200)(継続犯(201))。支配下(制御可能状態)に置いている間、犯罪が継続すると

---

(196)　鈴木義男「航空機の強取等の処罰に関する法律について」曹時22巻８号１頁、18頁(1970)、奥村誠「航空機の強取等の処罰に関する法律について」警察学論集23巻５号33頁、37-38頁(1970)、大村・前掲注(180)35頁。

(197)　鈴木・前掲注(196)23頁。

(198)　強盗罪においても同罪の財産犯性を強調するのは相当ではなく、他人の生命又は身体への危険の大きさが考慮されているという説明に鈴木・前掲注(196)19頁(大村・前掲注(180)36頁も参照)があるが、やはり不法領得の意思を不要とするには「運航支配」の要件の追加が必要であった。

(199)　奥村・前掲注(196)38頁。客観的行為態様は強取と運航支配とで変わらない(鈴木・前掲注(196)22頁)。しかし、そうなのであれば、あえて「強取」を要件として入れる必要はなかったようにも思われる。また、輸送役務を受けた場合に２項強盗罪が成立し得るが、同罪は運航支配罪に吸収される(安西・前掲注(149)274頁)。

(200)　大村・前掲注(180)41頁。その意味では、状態犯だと解し得る強盗罪で使われる強取の文言を用いることには問題があるかもしれない。

(201)　安西・前掲注(149)275頁。

いう理解は、サイバー攻撃との関係では、ログインしていつでも不正な操作ができる状態になっている期間、犯罪が継続するという理解をも導き得るが、その間、システムの可用性を低下ないし喪失させているとすれば、その思考は妥当なように思われる。

乗組員による行為も本罪で処罰される(202)。さらに、行為者が航空機内にいることを要しない(203)。運航支配罪は予備罪も処罰するが(法3条)、次に述べる要件の存在ゆえに、サイバー攻撃への対応が難しくなっている。すなわち、同罪の成立には、規定上、暴行若しくは脅迫を用い、またはその他の方法により「人」を抵抗不能の状態に陥れることが要求され、(最終的に機長の)反抗抑圧に向けた行為により運航を支配しないと本罪にあたらないので(204)、サイバー攻撃によるものが含まれないと解さざるを得ない。人の意思への働きかけなく勝手に制御権限を乗っ取る行為は本罪で捕捉できないのである。

サイバー攻撃による制御乗っ取りについて窃盗罪の成否を検討する余地があるかもしれないが、不法領得の意思が必要になるだけでなく、それをクリアしたとしても(205)、致死結果による加重が懸念されるような状況を作り出す可能性があるのに窃盗致死罪は存在せず、また後述の運

---

(202) 大村・前掲注(180)37頁。

(203) 奥村・前掲注(196)38頁。

(204) 暴行・脅迫の相手方は乗客等でもよいが、最終的に機長の意思の制圧に向けられる行為が要求される(平野ほか編・前掲注(148)航空機の強取等の処罰に関する法律45頁〔戸田信久〕(青林書院、1983))。安西・前掲注(149)273頁も参照。暴行・脅迫はその他の方法による場合と異なり、相手方を抵抗不能の状態に陥れる必要はない、とするが、これは強盗罪において反抗抑圧を客観的要件として考えるか否かの問題と連動した見解の相違だといえ、(ここでは恐喝的行為との区別の必要性は薄いものの)むしろ抵抗不能ないし反抗抑圧は客観的な要件として要求されるべきように思われる。

(205) 自動車窃盗の事案と比較すれば、航空機の無断使用につき、不法領得の意思が欠けることは通常は考えられないとも思われる(平野ほか編・前掲注(148)航空機の強取等の処罰に関する法律48-49頁〔戸田信久〕)。ほかに本罪の強取につき、不法領得の意思が広く肯定されてきていることに言及するものに大村・前掲注(180)39頁。

航阻害罪と同じ最高刑の窃盗罪でしか対応できないことには疑問があり得る。

これは、つまるところ、運航という現象が最終的には機長の意思にかからしめられているという前提をおいていることに起因する。機長の意思の完全な制圧→運航支配、意思の不完全な制圧→(次に述べる)運航阻害という対応関係それ自体が、(意思に働きかけない)サイバー攻撃による運航支配の場合をうまく捕捉できない原因となっている。上記前提をもはや採るべきではないとすれば、その場合には、サイバー攻撃を行為態様に付加した、運航支配罪の立法が必要になるかもしれない。

第２目　航空機の運航阻害罪

運航阻害罪は業務妨害罪の加重規定(業務妨害罪の特別法[206])である。偽計・威力業務妨害罪の最高刑が３年で電子計算機損壊等業務妨害罪の最高刑が５年であるのに比し、１年以上10年以下の懲役と、法定刑の上限も下限も引き上げられている点が特徴的である。航空機の特殊性を踏まえたものであるとはいえ、こうした傾向は重要インフラの保護を考えるにあたって参考になる。

運航阻害罪における偽計については、刑法上の偽計業務妨害罪と同一に解され[207]、対人的攻撃が主に想定されていたようである[208]。サイバー攻撃も何らかの形で最終的に人に発見されるという意味で、対人的要素を有する陰険な手段であるというのであれば、偽計の概念にサイバー攻撃を含むと解する余地もあり得なくはない[209]。しかし既に刑法上、偽計業務妨害罪と電子計算機損壊等業務妨害罪とが異なる法定刑をもって分けられている現状を考えると、その差異を無視すべきではないともいい得る。そうだとすると、電磁的記録の損壊等による運航阻害を行為態様として追加するか、進んで「電子計算機損壊等運航阻害罪」を現在の運航阻害罪よりもより重い犯罪として規定するべきかもしれな

⑵⑹　奥村・前掲注⑴⑼⑹45頁。

⑵⑺　奥村・前掲注⑴⑼⑹45頁、46頁。

⑵⑻　急病や事故を装って機長を欺く等。奥村・前掲注⑴⑼⑹45頁、46頁。

⑵⑼　第３章第３節第３款第４項参照。大谷ほか・前掲注⑷⑶23-24頁〔古田佑紀発言〕の議論参照。

い。これは立法論的な課題になり得る。

ここでいう運航阻害とは、運航支配には至らないが、正常な運航が現実に障害されることを要し、目的地への到着を遅らせた場合や航空機の高度や速度の変更等がその例だとされる(210)。運航阻害は、抽象的危険犯たる業務妨害罪における業務の妨害よりも厳格なものだと解されている。これは、運航支配罪が強盗罪よりも不法領得の意思を不要とする観点から処罰範囲を拡げているのに対し、運航阻害罪においては、元々の偽計や威力による業務妨害の概念が広く解されていることや、法定刑が重いことを踏まえて、運航の阻害は運航業務の妨害よりも狭く解され、かつ未遂も処罰しないことにした(211)、という沿革に由来する。もっとも、運航阻害に至らない場合は偽計業務妨害罪での処罰は可能だとされているから(212)、業務の妨害がサイバー攻撃によって惹起された場合には電子計算機損壊等業務妨害罪又はその未遂罪で処罰が可能だと解される。それゆえ、実質的には運航阻害「未遂」として、電子計算機損壊等業務妨害(既遂あるいは未遂)が位置づけられることになる。サイバー攻撃以外の行為態様への波及効果を有する重い法定刑を有する運航阻害罪の処罰の早期化を、同罪の規定の「阻害」を「妨害」にするとか、未遂処罰規定を入れる等といった手法で実現することも考えられるが、基本的にはサイバー攻撃以外の部分について立法事実による正当化がないから、採るべきではないと思われる。

なお、運航支配罪も運航阻害罪も、運航権限を有する機長には適用されず、内部者たる機長の行為に対しては、監禁罪、業務上横領罪、背任

---

(210) 鈴木・前掲注(196)30頁、奥村・前掲注(196)48頁、安西・前掲注(149)281頁。電車に対する攻撃であったために偽計業務妨害罪に問われるにとどまったが、改造した防護無線通信装置から電波を発射してJR東日本の列車に設置してある防護無線通信装置に同電波を受信させ、列車を緊急停止させたり、発車を見合わせたりしてその運行を遅延させる行為(東京地裁八王子支判平成９年７月４日判タ969号278頁)は、運航阻害の想定する状況を充たしているとも評価し得る。

(211) 鈴木・前掲注(196)31頁、奥村・前掲注(196)45頁、47頁。

(212) 奥村・前掲注(196)48頁。

罪、航空法上の機長職権濫用罪や、国外移送目的拐取罪や国外移送罪等の成立が考えられる(213)。これらの犯罪により既に相当重く処罰することが可能ではあるが、機長の不法な行為について重い罰則を設けることも考えられなくはない(214)。

さらに、航空機の運航を担うシステムに対するサイバー攻撃が内部者により行われる場合には、甚大な被害が生じる危険が相当程度早期の段階で発生し得ることを考慮すると、保護対象たる航空機の運航を担うシステムを特定しつつ、これを「みだりに操作する」行為を処罰することの可否を議論の俎上に乗せることが可能かもしれない(→第１款第２項第２目における新幹線特例法の議論参照)。

第４項　小括

以上、航空インフラについては、運航支配(阻害)罪のように、制御乗っ取り(攪乱)に直接対応できる重い犯罪類型を有していることがわかったものの、それ自体、サイバー攻撃に対応させる必要がある部分があるということもわかった。サイバー攻撃の捕捉可能性についての検討結果をまとめると表３のようになる。

これらの知見を活かしつつ、さらに将来的に問題となり得るコネク

表３　運航支配罪、運航阻害罪、電子計算機損壊等業務妨害罪の整理

	中間結果を含めた行為態様	構成要件的結果	現状分析
運航支配罪	機長の反抗抑圧に向けた行為		サイバー攻撃を捕捉できない
運航阻害罪	偽計また威力	阻害は業務妨害における妨害よりも厳格な概念	偽計にサイバー攻撃を入れられるかが解釈上の問題
電子計算機損壊等業務妨害罪	電子計算機損壊等	業務妨害	受け皿として機能し得る

(213)　鈴木・前掲注(196)20頁、大村・前掲注(180)37頁。

(214)　大村・前掲注(180)37頁。

ティッドカーシステムへのハッキングについて、検討する。

第４款　コネクティッドカーシステムの安全

以上、刑罰規定で厳重に規制されてきている交通インフラをみてきた。ここでは、サイバー・フィジカル・セキュリティの維持の観点から制御乗っ取りや制御の攪乱が起きることを想定し、コネクティッドカーシステムに対するサイバー攻撃に対する法的対処の方法を考える。既にコネクティッドカーの制御がリモートで乗っ取られる等するリスクが指摘されているから(215)、議論する必要性が大きい。コネクティッドカーにも様々な定義があり得るところ、ここでは実害から逆算する形で、ネットワーク接続により一定の制御が可能な自動車のことをいうものとしておきたい。

ここでも他の交通インフラと同様に公共危険犯から個別具体的な制御に対する攻撃、及びサイバー犯罪対策規定の有効性を議論したい。

第１項　往来・交通危険罪

第１目　往来妨害罪の不十分性

道路交通の安全は、まずもって刑法上の陸路についての往来妨害罪（刑法124条）で図られている。しかし、往来妨害罪は、陸路（公衆の通行に供される陸上の通路（道路法等にいう道路に限られない））に対する往来妨害惹起行為の全てを処罰するわけではなく、物理的に損壊または閉塞する場合のみを処罰する。道路を掘り返す行為等が損壊の例として、障害物の設置行為が閉塞の例として挙げられるが、サイバー攻撃の結果とし

(215)　コネクティッドカーのサイバーセキュリティについては、2020年６月24日に採択された国連の規則（UNECE, Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system Submitted by the Working Party on Automated/autonomous and Connected Vehicles（2020. 6. 23）（https://www.escrypt.com/sites/default/files/2020-07/ECE-TRANS-WP29-2020-079-Revised-2.pdf）、UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles（http://www.unece.org/?id＝54667））や、さらに西貝・前掲注(147)48頁にて参照した文献も参照。

て、物理的な環境の状態変更が問題になる場合は相対的に多くないだろう。水路について述べたところと同様、行為態様を無限定にすることには、サイバー攻撃以外の行為態様をも全て含むことになりかねず、慎重な検討を要する。

また、本罪は、人等の円滑な通行を保護しようとするものであって、相当な時間にわたっての行為(損壊・閉塞)の効果の継続を要求する[216]。ハッキングや不正な指令の送信による権限ある者による制御の妨害と、事象として一対一対応しているかも定かではない。例えば、車がやっと通れる程度の不法駐車が往来妨害罪になりうるかにも争いがある[217]。サイバー攻撃で不正に自動車を停止させることは可能かもしれないが、ここで問題としているのは、瞬間的にであっても、制御が乗っ取られたり、攪乱されたりする(ことによる交通への危険が発生した)場合の処理である。自動車停止後の状況の継続を問題とする往来妨害罪とはやや当罰性を議論する視点がずれているともいえる。それゆえ、往来妨害罪やその拡張的な立法論を用いたサイバー攻撃への対処には疑問が残る。

第２目　道路の種類に応じた往来・交通危険罪

特別法をみると、往来危険罪や交通危険罪が、道路の種類に基づいて、または標識の効用の保護を通して規定されている。

例えば、強力な処罰規定として自動車道における自動車の往来危険罪がある(道路運送法100条１項)。本罪では、その行為態様を問わず(「その他の方法」[218])処罰可能である(５年以下の懲役)。自動車事故が発生する可能性のある危険な状態を現実に作出することを要する具体的危険犯である[219]。既遂時期の考え方は、刑法125条の往来危険罪と同じだとされ、自動車の衝突・転覆などの事故発生の可能性ある状態の作出で必要十分である[220]。その意味で、サイバー攻撃による制御乗っ取りや制御攪乱行為を捕捉できるかもしれないが、「危険の発生」にあたるか否か、

216　『大コンメンタール 第３版 第７巻』202頁〔渡邉一弘〕。

217　『大コンメンタール 第３版 第７巻』202-203頁〔渡邉一弘〕。

218　自動車道や標識の本来の機能の一部または全部を失わせる行為で損壊以外のものが含まれる(安西温『改訂 特別刑法 ２』70頁(警察時報社、1986))。

219　安西・前掲注218)70-71頁。

解釈上の不透明性がなお残る。さらに、ここでいう自動車道は、「専ら自動車の交通の用に供することを目的として設けられた道で道路法による道路以外のもの」(道路運送法２条８項)と定義されており、想定される道路が限定される。

道路法にいう道路というのは、高速自動車国道、一般国道、都道府県道、市町村道である(道路法２条１項、３条各号)。このうち、高速自動車国道以外については、刑法上の往来妨害、往来危険罪の特別法としての[221]、道路の効用侵害又は交通危険罪が適用され(道路法101条、３年以下の懲役又は100万円以下の罰金)、高速自動車国道については高速自動車国道の効用侵害又は交通危険罪が規定されている(高速自動車国道法26条、５年以下の懲役又は200万円以下の罰金)。両罪はほとんど同じ規制であり、両罪ともに、行為態様が客体たる道路それ自体の損壊または客体たる道路の付随物の損壊または移転である点で共通し、いずれも道路における交通事故発生の可能性のある危険な状態を現実に作出することを要する具体的危険犯だと解されている[222]。また、高速自動車国道については重く、かつ未遂犯も処罰される(高速自動車国道法26条２項)[223]。

以上からは道路の性質に応じた処罰の軽重、及び早期化処罰の工夫をうかがうことができる。一方で、行為態様が上述のように限定されているため、サイバー攻撃が含まれると解することは難しい。

そこでより一般的に抽象的危険犯を用いた犯罪類型である道路法43条

---

[220] 伊藤榮樹＝小野慶二＝荘子邦雄『注釈特別刑法 第６巻Ⅰ 交通法・通信法編 新版』656頁-657頁〔江藤孝〕(立花書房、1994)。もっとも、道路運送法上の自動車道における往来危険罪は鉄道についての往来危険罪(刑法125条１項、２年以上の懲役)よりも法定刑がかなり軽くなっており、法定刑の下限が１月の懲役であることから、危険の発生についてより緩やかな解釈がなされる可能性もある。

[221] 安西・前掲注[219]20頁、22頁。具体的に行為態様が定められている点をみると往来妨害罪(刑法124条)の特則という(道路法令研究会『改訂５版 道路法解説』741頁(大成出版社、2019))方がよいかもしれない。

[222] 安西・前掲注[219]21頁、23頁。道路法令研究会・前掲注[221]742頁は道路における交通に危険な状態の発生が必要であり、現実に道路の交通に支障が生じたことは不要だとするが、侵害犯ではない点で本文の理解と共通する。

２号違反の罪（道路法102条３号）をみてみると「みだりに道路に土石、竹木等の物件をたい積し、その他道路の構造又は交通に支障を及ぼす虞のある行為」をした者は、１年以下の懲役又は50万円以下の罰金に処せられる（道路法102条３号）。客体は高速自動車国道か否かを問わない。本規定は、道路全般が客体になっており、また現実に交通の危険を発生させることを要しない抽象的危険犯だと解されており(224)、行為態様もその他交通に支障を及ぼす虞のある行為を包括的に捕捉しているとも読むことができ、サイバー攻撃さえも含むと解し得る。もっとも、物件のたい積等の例示されている行為から明らかなように、妨害電波の送信等をも含むと考えて立法された航空危険罪とは異なるし、不特定多数人の生命・身体等への危険を発生させる行為を可能にし得るサイバー攻撃を処罰するものとしては法定刑が軽すぎるかもしれない。

以上からすると、サイバー攻撃をも行為態様に含み得るものとして、まず自動車道における往来危険罪は自動車道という道路の種類に着目して規制しようとしているにとどまる。電車に関しては路線の種類を問わず往来危険罪が存在することと対比させて考えてもみると、自動運転・コネクティッドカー時代においては、道路の性質と関係なくリモートで不特定多数の自動車の制御が乗っ取られ、又は攪乱させられ得るとすれば、こうした法状況には不足があるといえるかもしれない。また、道路法上の犯罪についても、捕捉範囲を広く解することは可能であろうが、

---

(223)　より厳格な制裁をもって臨んでいる理由として、高速自動車国道が全国的な自動車交通網の枢要部分を構成し、政治・経済・文化上特に重要な地域を連絡する性質を有するという、同国道の重要性が指摘されているが（道路法令研究会・前掲注(221)742頁-743頁）、事故発生時の事故の大規模化のおそれも指摘できるかもしれない。

(224)　安西・前掲注(219)21頁。一方で、道路が一般交通の用に供される公共の施設である点を考慮し、道路の効用を保護する規定だという理解もある（道路法令研究会・前掲注(221)373頁）。この理解は、当該犯罪を公益目的に使われる道路の効用を侵害する罪と捉えるものであり、交通危険罪的な議論と距離を置くことで、（それ自体の妥当性について議論はあり得るものの、）軽い法定刑を説明し得る。

今度は、法定刑や行為態様の書き方については慎重な吟味が必要である。

第３目　信号機等の効用侵害罪

この点、道路について限定をしない、つまり道路運送法上の自動車道も道路法上の道路も含む形で広く一般交通の用に供する場所[225]における交通危険罪が道路交通法115条に規定されている（５年以下の懲役又は20万円以下の罰金）。道路交通法は、全体として道路交通の安全を保護するものであるところ（法１条参照）、同罪の保護法益はそのうちの信号機、道路標識または道路標示の効用である[226]。ここでいう信号機等（法２条１項14号から16号）は有体物であることが前提とされているだろう。信号機を操作（信号の表示の変更や停止[227]）・損壊（有形的作用による効用侵害[228]）、又は公安委員会が設置した道路標識若しくは道路標示を移転（他の場所への移動[229]や標板の方向の変更[230]）・損壊して、これらの効用を害

---

[225] ただし、立ち入りの管理が厳重になされていて、内部で別途交通規制が敷かれている会社の構内のような、不特定多数の自由に通行できないような場所はこの概念から除かれるとされ、やや当てはめに流動性があることには注意（村上尚文『刑事裁判実務大系４－ｉ　道路交通(1)』５頁-14頁（青林書院、1993）。

[226] 平野龍一＝佐々木史朗＝藤永幸治編 『注解特別刑法１　交通編(1) 第２版』道路交通法977頁〔浅野信二郎〕（青林書院、1992）、横井大三＝木宮高彦『註釈道路交通法（再訂版）』567頁（有斐閣、1967）、宮崎清文『新版 注解 道路交通法』837頁（立花書房、1992）、交通法令実務研究会編『改正 条解 道路交通法』444頁（警察時報社、1979）。

なお、道交法76条１項・２項違反の罪（道交法118条１項６号）が、信号機や道路標識等の効用を保護するために、これら、及びこれらに類似する物件（１項）、並びにこれらの効用を妨げる物件（２項）の設置を禁止している。「設置」を道交法115条の損壊と捉えることは難しいという理解からは、76条１項・２項に違反して交通の危険を発生させた場合に重い法115条の罪で処罰できない点に不均衡があるとも指摘される（伊藤ほか・前掲注[220]457頁〔長井圓〕）。なお、１項の罪に類似する規定に刑法上の往来危険罪があるとされつつ、同罪は鉄道及びその標識に関連する場合のみを捕捉するから、道交法で補充する意味があるという指摘があり（木宮高彦＝岩井重一『詳解 道路交通法〔改訂版〕』207頁（有斐閣、1980））、往来危険罪の自動車版についての必要性を基礎づける議論になっている。

して、交通の危険を発生させると本罪にあたる。交通の危険の発生というためには、現実に危険が発生したことを必要とせず、道路における交通の危険の発生のおそれの惹起で足りると解されている(231)。危険の発生の認識が故意として必要である(232)。危険発生のおそれという用語法はかなり抽象的であるが、信号機等の持つ機能の重要さに鑑みれば、容易に肯定し得るものかもしれない。

ここで信号機等は、自動車同士、自動車とその他の人車の動きを制御するための情報を各当事者に伝えることにより、交通の円滑化、安全を確保するという大きな社会的意味を持つものである。それゆえに、汚損等によって信号機等の表示する意味内容を不明にする場合も損壊に該当する(233)。こうした情報は自動運転・コネクティッドカー時代においては、システムへの実装上、必ずしも人の目に付く形ではなく、サイバー

---

(227)　伊藤ほか・前掲注(220)538頁〔長井圓〕、平野ほか編・前掲注(226)道路交通法977頁〔浅野信二郎〕、横井＝木宮・前掲注(226)567頁。さらに作動していない信号機を作動させる行為を含むとするものに道路交通執務研究会『18訂版執務資料道路交通法解説』1319頁(東京法令出版、2020)。

(228)　伊藤ほか・前掲注(220)538頁〔長井圓〕〔有形的作用による客体の形態の変更〕。単に効用侵害とするものに平野ほか編・前掲注(226)道路交通法978頁〔浅野信二郎〕、木宮＝岩井・前掲注(226)297頁、宮崎・前掲注(226)837頁、道路交通執務研究会・前掲注(227)1321頁。

(229)　伊藤ほか・前掲注(220)538頁〔長井圓〕。

(230)　平野ほか編・前掲注(226)道路交通法977頁〔浅野信二郎〕、横井＝木宮・前掲注(226)567頁、道路交通執務研究会・前掲注(227)1320頁。

(231)　横井＝木宮・前掲注(226)568頁、宮崎・前掲注(226)838頁、安西・前掲注(219)27頁、道路交通執務研究会・前掲注(227)1321頁。伊藤ほか・前掲注(220)457頁〔長井圓〕は、交通関与者を殺傷する等の交通事故が発生する危険があることを要する、とする。

(232)　伊藤ほか・前掲注(220)539頁〔長井圓〕、木宮＝岩井・前掲注(226)297頁、横井＝木宮・前掲注(226)568頁、道路交通執務研究会・前掲注(227)1321頁−1322頁。

(233)　宮崎・前掲注(226)837−838頁、道路交通執務研究会・前掲注(227)1321頁、安西・前掲注(219)26頁。汚物付着、ペンキ塗装、他の工作物等で遮蔽することによる視認困難・不能状態の惹起を含む(伊藤ほか・前掲注(220)538頁〔長井圓〕)。

空間上を行き交うデータとして表現されるかもしれない(人による確認が必要な場合、そのデータを参照して物理的に知覚可能な信号機等に情報を表示することになろう)。信号機の担う機能に関する情報が自動運行装置を含む多数の自動運転車の制御を担うCPSの一部になり得るわけである。その意味では、CPS時代においては、一方で有体物に信号機等を限定しているだろう現行法制には問題があり得るが、他方では、信号機等の効用侵害を、相当程度重く、最高刑５年の懲役刑で処罰していることには理由があると思われる。それゆえに道交法115条の罪は、刑法上の往来危険罪の特則と理解されているのだろう(234)。

もっとも、本罪の対象は、自動車自体へのハッキングというより、自動車を制御する外部情報の伝達手段に対する攻撃であるところ、そもそも、そのような区別が自動運転時代において重要なのか(上記の通り、自動車を多数制御する大きなシステムとして考えるべきではないのか)、また自動車自体へのハッキングそれ自体も往来ないし交通の危険を発生させるものであって、その点を処罰しなくてよいのか、という疑問が生じる。

第４目　今後の課題

以上、みてきたとおり、往来(交通)危険罪という意味では、道路毎やインフラ毎に特別な規制をもって臨んでいると整理可能である。もっとも、サイバー攻撃の危険性に鑑みると、コネクティッドカー時代においては、道路の種類と関係なく、コネクティッドカーが走行する道路における往来危険罪を整備しておく必要があるように思われ、この点を考えるのが本研究の課題になっている。

第２項　運「行」支配罪等の必要性

そこで、第３款第３項(航空機の運航支配・運航阻害罪)に対応する形で、IoTの塊といってもよいコネクティッドカーシステムに対する具体的な制御乗っ取りや攪乱について検討する。

第１目　自動運行装置の概念整理と不備に対する処罰

現在、AI・IoT技術の発展により、自動運転車の社会実装が期待されており、既に「自動運行装置」の概念が道路運送車両法に組み込まれて

(234)　安西・前掲注(219)26頁。

いる（道路運送車両41条２項、１項20号）。道路運送車両41条１項柱書は、国土交通省令に基づく保安基準[235]への適合性の維持を要求し、道交法62条は、保安基準に適合しないため交通の危険を生じさせるおそれ等がある整備不良車両の運転の禁止を定める。自動運行装置を用いる場合も道路交通法上の運転にあたり（道交２条１項17号括弧書[236]）、保安基準に適合しない自動運行装置を装備している整備不良車両の運転は処罰される（軽車両を除く車両等につき道交119条１項５号（過失犯の場合には法119条２項））。

第２目　無免許運転罪か運「行」支配罪か

もっとも、一定の通信を行いながら車両の運行を制御する以上、適式に自動運行装置を利用していても、サイバー攻撃を受けて思わぬ挙動を示すことがあり得る。サイバー攻撃者による制御乗っ取りも運転の概念にあたり得、その場合、同人には無免許運転罪が成立するものと解し得るが[237]、無免許運転罪では、制御乗っ取りの危険性を十分に捕捉できないように思われる。

すなわち、航空機の中に不特定多数人が存在するのと異なり、自動運転車の場合には、それぞれの自動車内の人数は少数ともいえるが、多数の自動運転車の暴走を惹き起こしかねない点や、車外といういわば安全地帯から攻撃が可能になっている点で、結局、航空機と同じく、不特定多数人の生命・身体の保護という観点から考察すべきである。ハイジャック防止法とパラレルに運「行」支配罪の検討を行う余地があるように思われる。その際には、既に運航支配罪の検討部分（第３款第３項第１目）で述べたとおり、「サイバー攻撃」を行為態様に含められるように工夫して立法する必要がある。

第３目　制御攪乱行為

GPSを用いて一定の自動制御を行うコネクティッドカーにおいて、

---

[235]　保安基準48条参照。告示等の詳細は国土交通省のHP参照。

[236]　これは確認規定だとされる（道路交通法研究会編著『注解 道路交通法 第５版』928頁（立花書房、2020））。

[237]　西貝・前掲注[147]49頁−50頁。

GPSのデータが不正に変更された場合には、直接に同車への制御への影響が出ることになり、そのような自動車も従前の自動車と一緒に道路を走行するということを前提とした議論をすべきことになる。GPSデータのネットワークからの不正入力による不特定又は多数の自動車の突然の暴走もあり得ないではないとすると、公共危険犯の活用が検討されるべきかもしれないし、あるいは航空インフラの保護(第３款)とパラレルに考えると、電子計算機損壊等業務妨害よりも重い運「行」阻害罪の新設が検討されてもよいかもしれない。

第３項　小括

コネクティッドカーシステムに対するサイバー攻撃に対するアプローチの方法は多彩である。よりよい立法を模索する際には、外国の規律も参考になり得る。ここでは、比較法的な検討の前提として、我が国における現状の複雑な法規制を整理してみたことになる。

第５款　ここまでのまとめと試論としての若干の展望

交通インフラを担うシステムに対するサイバー攻撃を用いた侵入自体に往来危険罪を使うことが難しい場合があり得る(第１節第１款第１項)。そこで、少なくともサイバー攻撃に関しては、往来危険の予備(準備)罪的な規定を新設することが検討されてもよいかもしれない。予備行為や準備行為については、それを一般的に処罰することも法技術的には可能であるが、その手法は刑事立法で避けるべき過剰処罰のおそれが生じることになる。そして、本研究で問題としているのは行為態様がサイバー攻撃である場合に限られる。そうすると、例えば刑法典でいえば通貨偽造準備罪(刑法153条)があり得る予備行為のうちの「器械又は原料」の準備行為を限定して処罰するように、サイバー攻撃に行為態様を限定した形での予備的行為を考えていくことになるだろう。それは、サイバー犯罪の側から見れば、往来危険発生目的のハッキング罪の要否の問題でもある。

さらに別のインフラについても検討し、比較法研究の素地を構築していく。

第２節　電気・ガス・水道インフラの保護

国外における水道インフラへのサイバー攻撃の事例を紹介したよう

に、電気・ガス・水道(以下「電気等」という)といった生活上必須のインフラに対するサイバー攻撃による操業停止等の行為も、CPSのセキュリティの観点から考察する必要がある。

電気等のインフラに対するサイバー攻撃によってデータを権限なく改変して、サーバの停止等を惹起させればインフラ事業者の業務を妨害したとして電子計算機損壊等業務妨害罪が成立することは疑いがないだろう。

しかし、ここで問題としているのは、こうしたインフラに対する攻撃の結果、例えば、直接に(水道に過剰な消毒液が混入してそれを飲んだ者が死亡する事例)、または間接に(通電停止により、点滴装置が停止して必要な治療が行えず、患者が死亡する事例)、不特定又は多数の者の生命に対する危険が発生する場合に、電子計算機損壊等業務妨害罪だけで十分な処罰が可能か、ということである。

上記の死亡事例を考えたときに、殺意や傷害の故意を認められるのであれば、殺人罪や傷害罪等の生命・身体を保護する罪で処罰できるだろうが、それもない場合にどのように考えるべきか、ということを検討したい[238]。

そこで、それぞれのインフラの刑法、及び特別法における保護態様をみてみることにする。検討対象には、刑法上の犯罪類型だけでなく、国民の生活に必須となる電気、ガス、水道の安定供給を一つの趣旨とする電気事業法、ガス事業法、水道法上の犯罪類型も含まれる。電気事業、ガス事業ともに公益事業であり、一般の利用者を保護するための事業の監督だけでなく、技術的にガス、電気それぞれにある種の危険を伴う面もあるから、保安的な見地から設備上の監督をするという側面を有している[239]。電気事業法とガス事業法とでは罰則に関する規制態様が類似するので、電気事業法を主に分析していく。

238　さらに、放火罪や出水罪(水利妨害罪も含む)に関連する規定も問題になり得るが、これらはインフラというより、個人のスマートホームに対するサイバー攻撃においても問題になり得るものである。そこで、本稿では、ひとまず、インフラに焦点を当てていると思われる刑法及び事業法上の罰則を検討することにしたい。

第１款　電気事業法

ここでは新旧の電気事業法を検討していく。旧電気事業法というのは、明治44年に制定された、事業規制と保安規制の両面からなる法律のことをいう。本研究では、電気工作物の安全を図る罰則について主に検討したいので、検討対象を下記で紹介する規定に限定する。旧電気事業法の廃止から現行の電気事業法への制定や現在に至るまでの詳細な行政規制について詳しくは電力政策研究会編『電気事業法制史』を参照されたい。

第１項　旧電気事業法

電気事業は一般公衆の日常生活及び産業に欠くべからざるものを供給する事業であるから、電気工作物に対する各種の障害をできる限り防止することが肝要である(240)。こうした観点から、本研究においてみる旧電気事業法の関連規定は以下のものである。電気事業法は明治44年に制定されたが、当時は18条、19条にあった関連規定は、昭和６年改正により、下記の33条と34条に移された。

旧電気事業法
法33条１項　電気工作物(241)ヲ損壊シ、之ニ物品ヲ接触シ又ハ其ノ他ノ方法ヲ以テ電氣ノ供給又ハ使用ヲ妨害シタル者ハ五年以下ノ懲役又ハ三千圓以下ノ罰金ニ処ス
２項　前項ノ未途罪ハ之ヲ罰ス
法34条　電気事業者ノ承諾ヲ得ズシテ濫ニ電気工作物ノ施設ヲ変更シタル者ハ五百圓以下ノ罰金又ハ科料ニ処ス

(239)　第18回衆議院通商産業委員会議録第３号（昭和28年12月４日）９頁〔通商産業事務官（公益事業局長）中島征帆発言〕。
(240)　遠藤後一『電気事業法律論 上巻』431頁（電気協会、1928）。
(241)　「電気工作物」とは電気の供給又は使用のため施設する水路、貯水池、基部、機械、電線路その他の工作物であって、電気事業の用に供する物である（旧電気事業法２条１項）。

第１項　電気供給妨害罪

法33条の結果である電気の供給妨害は一般公共に重大な障害を与えることであるがゆえに、本条の罪は公共危険犯だとされる(242)。

本罪は、電気窃盗罪や器物損壊罪(工作物の損壊)のように、刑法で捕捉できない公共の利益を損なう行為を捕捉するために設けられた(243)。

本罪の法定刑は刑法上の電気漏出罪(刑法118条１項)のそれよりも重い。この点につき、立法過程においては、電灯営業や電気鉄道に対する電気の供給の停止による不測の被害や公安上の懸念があることから、電気漏出罪ではなく、むしろ刑法119条から126条の公共危険犯の法定刑を参考にしたのであり、それにより権衡がとれている、と説明された(244)。

「其ノ他ノ方法」とは、方法を問わない趣旨である(245)。もっとも、当分使用を休止している電線を切断する場合、構成要件的行為として電気工作物の損壊が認められても、電気の供給妨害という結果(246)が発生していないので既遂犯は成立せず、切断目的に留まる場合には器物損壊罪の成立が、領得の目的がある場合(弱電流電線の窃盗犯が電線窃盗では多いが、知識を有する者による身体に対する保護を講じ、器具を用いての高圧線の切断盗取の事案もあるとされていた(247))には窃盗罪の成立が認められ得るにとどまる(248)。

(電気の供給に障害があるべきことの認識を要する)故意犯である(249)。方法を問わないので、電気工作物と全然別個の他の工作物を設置して、そ

---

(242)　遠藤・前掲注(240)434頁、遠藤後一「電気事業及瓦斯事業法」『現代法学全集14』391頁、折原泉「電気並に電気施設に関する犯罪に就て」司法研究第12輯報告書集３号１頁、31頁(1930)。

(243)　電力政策研究会編『電気事業法制史』86頁(電力新報社、1965。以下『電気事業法制史』として引用)。遠藤・前掲注(240)434頁。

(244)　第26回帝国議会衆議院電気事業法案委員会第４号(明治43年３月14日)19頁〔中谷弘吉発言〕。

(245)　遠藤・前掲注(242)391頁、電気協会『電気事業法規解説』388頁(1933)、『電気事業法制史』86頁、折原・前掲注(242)31頁も参照。

(246)　当然結果の認識も必要である(電気協会・前掲注(245)388頁)。

(247)　折原・前掲注(242)31頁。

れによって電気の供給が妨害された場合にも客観的要素を充たすことになるが、その場合、故意が欠けることが多いと指摘されている(250)。

第２項　電気工作物施設変更罪

法34条の罪は、最も起こりやすい犯罪だと評されていた(251)。本罪を処罰する理由は、電気の知識のない者が電気事業者の施設した設備を無断で変更することによって発生し得る(252)、火災や傷害の危険に求められていた(253)。公共危険の予防のための規定だと位置付けられている(254)。施設の変更行為それ自体は中立的であると考えると、「電気事業者の承諾を得ないこと」と「濫に」の２要件により、行為の違法性を表現した規定になっていると評価される。ここで問題になっている電気工作物の施設の変更行為については、羅列的に紹介されることが多い。立法過程においては、既に需用者の下に引いてある電線路を同人が勝手に延長する行為が施設変更罪にあたり得るとされていた(255)。

第１目　客体としての「電気工作物の施設」

法文に出てくる概念の定義からみると、電気工作物とは、旧電気事業法２条において、「電気の供給又は使用の為施設せられる水路、貯水池、器具、機械、電線路(256)其の他の工作物にして電気事業の用に供するもの」と定義される。電動機、電線、電柱等がこれにあたる(257)。

電気工作物の所有権が自己にあるか否かを問わないので(258)、器物損

---

(248)　鷲山半之助『判例実例挿入特別法罰則適用総鑑』1142頁（新光閣、1936）〔未遂犯にもならないという〕。鷲山は、罪数について、窃盗罪と本罪とは観念的競合、器物損壊罪と本罪とは法条競合の特別関係にある（本罪が優先適用される）と解している。電気協会・前掲注(245)388頁も参照。一方で、器物損壊と本罪とが観念的競合になると解するものに折原・前掲注(242)31頁。

(249)　遠藤・前掲注(240)436頁。

(250)　遠藤・前掲注(240)437頁。

(251)　鷲山・前掲注(248)1142頁。

(252)　『電気事業法制史』86頁。

(253)　電気協会・前掲注(245)388頁−389頁。折原・前掲注(242)34頁。

(254)　折原・前掲注(242)34頁。

(255)　第26回帝国議会衆議院電気事業法案委員会第３号（明治43年３月12日）〔中谷弘吉発言〕。

壊罪とは別の制度趣旨を有している。

電気工作物にあたるか否かの判断においては、判例上、分離の容易性が重要である。制度趣旨には、知識不足な者の行為の危険性が指摘されていたが、取り外す際の特別な知識の要否は重要ではない[259]。まず、電灯球は電気工作物ではない。電球は取付けにより接合するに止まり、この物体を損壊しないで自在にこれを分離し又は他の電灯球との取替えができることを通常とし、その取外し取替え等に関しては別に技術上の知識を要しないことが理由として挙げられた[260]。これに対して、電灯線(これは電気工作物である)の末端に取り付けられる「ソケット[261]」について、用法上、電灯線と合して一体をなし分離すべからざる関係を有するものであることを理由に電気工作物であると判断された[262]。知識がなくても取り外しできる、という主張もなされたが、その点については判断がなされず、上記の結論に至っている。

第２目　変更

変更の概念は文言から基準が得られない[263]。模様替のことだとされることもあるが、より抽象的なパラフレーズのようにも思われる[264]。よって例示されているところをみると、移転や取外しが変更に含まれる[265]。

256　旧電気事業法２条２項によれば、電線路とは「前項に於いて電線路と称するは電気の伝送に用ふる電気導体及之を支持し又は保蔵する工作物」のことをいう。

257　茂見義勝『特別法犯捜査要綱』189頁(法制時報社、1939)。

258　『電気事業法、その他』(オーム社、1932)「電気事業法改正法律の説明」内38頁参照。

259　大判大正15年２月24日刑集５巻61頁。

260　大判大正６年10月８日大審院判決録第13巻1050頁。

261　電灯用として屋内に施設する電線と電球との間に介在して電流の交通又は遮断の用に供せらるべき装置をいう(大判大正15年２月24日刑集５巻61頁)。

262　大判大正15年２月24日刑集５巻61頁。

263　茂見・前掲注257190頁。

264　折原・前掲注242)32頁。

さらに電気工作物の増設は変更にあたる(266)。例えば従来の工作物以外に新たに電燈線を引き、別個の場所に一の電燈を増設した場合である(267)。また、電気工作物の「施設」が変更の対象となっているので、電気工作物自体に変更を加えなくても、これに近接する他の工作物を変更し、その施設状況に変更を及ぼす場合もなお、施設の変更に該当する(268)。

第３目　その他の要件

電気工作物の施設の変更行為が電気事業者の承諾のないものであれば、本罪が成立するという説明がある(269)。「濫に」を実質的違法要素だと評価していることが前提となろう。

なお、電気工作物の変更行為が必ずしも電気窃盗に結びつくわけではないように思われるものの、同行為と電気窃盗罪との関係は牽連犯になるとするのが判例である(270)。

さらに、本条違反の結果、失火事件になることが多い(271)。この点は、サイバー・フィジカル・セキュリティを保護する観点からは参考になる。

---

(265)　折原・前掲注(242)32頁。

(266)　電気協会・前掲注(245)389頁。

(267)　大判大正６年12月４日刑録23輯1486頁。ただし、単に電球を取り替えるような事案は変更にあたらない(大判大正６年10月８日(前掲注(260))。さらに、２個以上の電燈燈火の用に供する目玉の類の設置は施設の変更にならないと解するものがある(折原・前掲注(242)33頁)。その理由について、折原は、こうした事案を電気盗用的な事案と理解しつつ、本罪は不法な施設変更を処罰するものであって、電気盗用の目的の有無を問わない罪であるからと説明する。

(268)　電気協会・前掲注(245)389頁、折原・前掲注(242)34頁。

(269)　茂見・前掲注(257)190頁。

(270)　大判大正10年10月14日刑録27輯23巻629頁〔ある会社により設備された電灯を消さずに、別に同社により供給されていた電燈用コードに電球が付いた電燈用コードの先端を裁縫用の針を使って接着して点灯させて、契約以外の電気を盗用した事案〕。

(271)　折原・前掲注(242)34頁。

第２項　現行の電気事業法

第１目　総説

現行の電気事業法は、戦後の法規制の混乱期を経た上で、新法(昭和39年法律170号)を作る形で制定された。本法は、電気事業の国民生活及び産業活動における不可欠性、非代替性、その高度な公益性を前提としつつ、我が国の経済の成長をエネルギーの観点から支えるため、電気の安定供給を維持することをその制度趣旨とする(272)。

電気はその物理的性質上、その取り扱いいかんによっては相当の危険ないしは障害を伴うものであり、保安面から電気工作物の規制が必要である(273)。罰則は、この種の規制の目的を担保するものと位置づけられよう。

第２目　電気事業法115条の罪

本研究の目的に関連する罰則をみてみると、現行の電気事業法には発電等を妨害する罪として法115条の罪がある。

> 第115条　電気事業の用に供する電気工作物を損壊し、その他電気事業の用に供する電気工作物の機能に障害を与えて発電、変電、送電又は配電を妨害した者は、５年以下の懲役又は100万円以下の罰金に処する。
> ２　みだりに電気事業の用に供する電気工作物を操作して発電、変電、送電又は配電を妨害した者は、２年以下の懲役又は50万円以下の罰金に処する。
> ３　電気事業に従事する者が正当な理由がないのに電気事業の用に供する電気工作物の維持又は運行の業務を取り扱わず、発電、変電、送電又は配電に障害を生ぜしめたときも、前項と同様とする。
> ４　第１項及び第２項の未遂罪は、罰する。

(272)　第46回衆議院本会議第16号(昭和39年３月24日)20頁以下〔通商産業大臣福田一発言〕。

(273)　第46回衆議院本会議第16号(昭和39年３月24日)20頁以下〔通商産業大臣福田一発言〕。

罰則を設けた趣旨は、電気が国民生活及び産業活動に必要不可欠である点に求められる[274]。行為態様と結果を整理すると下記の表のとおりである。

本罪を理解する上で重要な概念となる電気工作物は、電気事業法２条１項18号において「発電、変電、送電若しくは配電又は電気の使用のために設置する機械、器具、ダム、水路、貯水池、電線路その他の工作物（船舶、車両又は航空機に設置されるものその他の政令で定めるものを除く。）をいう。」と定義されている。

１項、２項の罪の主体は問わない[275]。これらの罪に関しては、構成要件的行為を行うだけで発電等の妨害という結果の発生がなければ、既遂犯の構成要件には該当せず、未遂犯の成立があり得るにとどまる[276]。２項の構成要件的行為が、「みだりに……操作」だけであるから、実効

	行為態様	結果	未遂	法定刑
１項	①電気事業の用に供する電気工作物を損壊し、②その他電気事業の用に供する電気工作物の機能に障害を与えて	発電、変電、送電又は配電の妨害	処罰	５年以下の懲役又は100万円以下の罰金
２項	みだりに電気事業の用に供する電気工作物を操作して			２年以下の懲役又は50万円以下の罰金
３項	（電気事業に従事する者が）正当な理由がないのに電気事業の用に供する電気工作物の維持又は運行の業務を取り扱わず	発電、変電、送電又は配電への障害の発生	不可罰	

[274] 資源エネルギー庁電力・ガス事業部 原子力安全・保安院『2005年電気事業法の解説』547頁（経済産業調査会、2005）。

[275] 資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注[274]548頁、549頁。

的な処罰範囲の限定のためにも、発電等の妨害の要件を侵害犯の結果と捉える必要がある。

結果の要件で列挙されている発電、変電、送電又は配電とは、電気の供給のすべての段階をいうもので、発電設備から需要家の引込み口の責任分界点までを含む[277]。

(1)　1項妨害罪

1項の行為のうち、①の「損壊」とは、広義の毀棄の一種であって、一部を破損することをもって足り、必ずしもその破損によってその電気工作物の効用を全く不能にすることを要しない[278]、とされる。器物損壊罪(刑法261条)においては、損壊しか行為態様がないために、効用侵害をも損壊にて捕捉する要請が強かったが、機能障害を同時に捕捉するこの規定ではそういう状況がない。②の機能障害で、損壊に至らない効用侵害が捕捉されていることからすると、損壊は物理的損壊に限られる趣旨に解すべきだと考える[279]。もっとも、損壊に物理的効用侵害を含むか否かで結論が異なることにはならない。

こう解すると、効用侵害は②のみにあたる。②の例としては、送電線に物を接触させる行為が挙げられている[280]。

なお、損壊、及び機能障害の双方で問題となり得る効用侵害は物理的なそれに限られると解すべきである。つまり、暴行脅迫による、あるいは(機能障害を発生させない態様での)汚物を付ける行為により心理的に利用できなくさせた結果として発電等が妨害されたとしても、威力業務妨害罪等にあたり得るにとどまり、本罪にはあたらないと解される[281]。

---

(276)　資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274)548頁。同書は、1項の罪を結果的加重犯だというが、侵害犯の誤りであろう。妨害の結果、人が死亡し、妨害と死亡との間に刑法上の因果関係が認められる場合で、かつ○○妨害致死罪というものが規定されていれば、その罪が、1項の罪の結果的加重犯だということになる。

(277)　資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274)549頁。

(278)　資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274)548頁。

(2) ２項妨害罪

２項の行為である「操作」とは、電気工作物本来の作動方法に従ってその工作物を運用することを意味し、「みだりに」とは、「正当な理由なく」と同趣旨であり、行為の目的、方法等が法律秩序の要求に違反する場合等、社会通念上公序良俗ないし条理に違反することをいうとされる(282)。真正不作為犯である３項があることとの関係では、２項の行為には作為のみが含まれると解すべきである。逐条解説によると、緊急避

---

(279) 既に述べたように、新幹線特例法２条１項の罪における「損壊」の概念（第４章第１節第１款第１項）や航空危険罪における「損壊」の概念（第４章第１節第３款第２項）も参照。

さらに、通信法分野における通信妨害罪の規定の解釈論は、本文のとおり損壊は物理的破壊をさし、機能障害をもって効用侵害を捕捉しようとしており、これが妥当だと思われる。通信妨害罪は現実に通信の妨害の発生を要件としない危険犯だと解されている点が異なるが、捕捉範囲の問題ではなく、損壊と機能障害が並んで規定されている場合の解釈上の棲分けの問題であるから、罪質は解釈論に影響を与えないと考える。

〔参照規定〕

・有線電気通信法第13条第１項

有線電気通信設備を損壊し、これに物品を接触し、その他有線電気通信設備の機能に障害を与えて有線電気通信を妨害した者は、５年以下の懲役又は100万円以下の罰金に処する。

・電波法第108条の２第１項

電気通信業務又は放送の業務の用に供する無線局の無線設備又は人命若しくは財産の保護、治安の維持、気象業務、電気事業に係る電気の供給の業務若しくは鉄道事業に係る列車の運行の業務の用に供する無線設備を損壊し、又はこれに物品を接触し、その他その無線設備の機能に障害を与えて無線通信を妨害した者は、５年以下の懲役又は250万円以下の罰金に処する。

(280) 資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274) 548頁。

(281) 通信法上の類似の規制と同様に解すべきである。通信妨害罪について伊藤榮樹＝小野慶二＝荘子邦雄『注釈特別刑法 第６巻Ⅱ 交通法・通信法編〔新版〕』411頁〔河上和雄〕（立花書房、1994）、郵政省電気通信監理官室『電気通信関係法 詳解 上巻』102頁（1973）。

難がここでいう正当な理由の一つだとされている(283)。しかし、「操作」には誰かの意に反するという要件が内在しておらず、この状態で「みだりに」を(ケースバイケースで判断される)違法性阻却事由がない場合であると解すると、構成要件のレベルでの限定機能がほぼ失われることになり妥当でないようにも思われる。もっとも、２項の罪(１項も同じ)が想定しているのは、行為そのものが公共の安全に重大な危険を及ぼす性質を有するものであるから(284)、(自動車の無免許運転罪と同様に、)原則としての不操作義務を肯定することで一応の当罰性の説明ができると思われる。

１項、２項の罪もいずれも故意犯であるから、行為、結果、因果関係の認識が必要であり、当然に、客体が電気事業の用に供する電気工作物であることの認識が必要である(285)。客観的に１項の罪に該当する行為をした場合においても、電気工作物であることの認識を欠く場合には、建造物ないし器物損壊罪の成立があるにとどまる(286)。

２項の犯罪と業務妨害罪とは観念的競合の関係にたつとされる(287)。公共危険犯と業務妨害罪との関係を考えさせられる議論である。すなわち、業務妨害罪の一つの加重類型に公共危険犯があると考えると１項、２項の罪を業務妨害罪の特別法(法条競合)と考えることも可能かもしれないところ、あくまで独立の犯罪類型だと考えれば観念的競合という理解に至りやすい。なお、業務妨害罪よりも軽い犯罪である２項の罪につ

---

(282) 資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274) 549頁。

(283) 資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274) 549頁。

(284) 資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274) 550頁(未遂犯処罰の正当化の文脈)。

(285) 資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274) 548頁、549頁。

(286) 資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274) 548頁。

(287) 資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274) 549頁。

いては、法条競合と解さないと、危険犯として運用されている偽計業務妨害罪について、みだりに操作する行為を偽計と捉える限り、２項の犯罪の存在意義がなくなってしまうように思われる。

(3)　３項障害罪

３項の罪は、電気事業に従事する者を身分とする身分犯の規定であり、サイバー犯罪の文脈では、一定の権限を有する内部者を主体とする犯罪である。そして、そうした身分を有していることにより、電気工作物の維持及び運行について類型的に作為義務が発生すると考えられたことから、真正不作為犯として規定されたと考えられる(288)。不作為の内容は、電気の正常な供給を確保するための保守、修理及び操作並びにこれに直接関連した作業(例えば、部品の取替え)のすべてをいうとされる(289)。保守の内容に、サイバーセキュリティの維持義務が含まれるか否かを問題にする余地があるが、含まれるとした場合においても、同義務違反と結果要件としての障害との刑法上の因果関係が必要であり、例えば、義務違反⇒第三者によるサイバー攻撃⇒障害について刑法上の因果関係を認められるかがなお問題となる。

第２款　ガス事業法

続いてガス事業法の検討に移る。ガス事業法の目的は、「ガス事業の運営を調整することによって、ガスの使用者の利益を保護し、及びガス事業の健全な発達を図るとともに、ガス工作物の工事、維持及び運用並びにガス用品の製造及び販売を規制することによって、公共の安全を確保し、あわせて公害の防止を図ること」にある(法１条)。

ここで問題となる犯罪行為に関連してみると、旧瓦斯事業法の罪(290)は現行のガス事業法の罪の一部を構成しているといえるから(旧瓦斯事業法22条の罪は現行ガス事業法192条１項に、旧瓦斯事業法23条の罪は現行ガ

(288)　資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274)549頁−550頁。

(289)　資源エネルギー庁電力・ガス事業部 原子力安全・保安院・前掲注(274)550頁。

(290)　鷲山・前掲注(248)1160頁は、旧瓦斯事業法22条、23条の罪と旧電気事業法とは同じに解してよいとしていた。

ス事業法193条の罪にそれぞれ対応する）、規定を紹介した上で、まとめて解説する。

旧瓦斯事業法
22条　瓦斯工作物の損壊其の他の方法を以て瓦斯の供給を妨害したる者は５年以下の懲役又は千円以下の罰金に処す
23条　瓦斯事業者の承諾を得ずして濫りに瓦斯工作物の施設を変更したる者は200円以下の罰金又は科料に処す

ガス事業法
192条
１項　ガス工作物を損壊し、その他ガス工作物の機能に障害を与えてガスの供給を妨害した者は、５年以下の懲役又は100万円以下の罰金に処する。
２項　みだりにガス工作物を操作してガスの供給を妨害した者は、２年以下の懲役又は50万円以下の罰金に処する。
３項　ガス事業に従事する者が正当な事由がないのにガス工作物の維持又は運行の業務を取り扱わず、ガスの供給に障害を生ぜしめたときも、前項と同様とする。
４項　第１項及び第２項の未遂罪は、罰する。
193条　ガス事業者の承諾を得ないでみだりにガス工作物の施設を変更した者は、50万円以下の罰金に処する。

第１項　ガス供給妨害罪

下記に示すとおり、電気事業法と同様の規制がなされている。

第１目　１項ガス供給妨害罪

ガスの供給を妨害するような行為は直ちに一般公共に重大な障害を与えるものであり、公共危険犯の一種であると解されている(291)。こうした評価には、ガスが国民生活及び産業活動に必要不可欠なものとなっている(292)という実態が前提にあるだろう。主体や方法は問わない。一般

	行為態様	結果	未遂	法定刑
1項	①ガス工作物を損壊し、②その他ガス工作物の機能に障害を与えて	ガスの供給の妨害	処罰	5年以下の懲役又は100万円以下の罰金
2項	みだりにガス工作物を操作して			2年以下の懲役又は50万円以下の罰金
3項	(ガス業務に従事する者が)正当な理由がないのにガス工作物の維持又は運行の業務を取り扱わず	ガスの供給への障害の発生	不可罰	

人も本罪を犯し得る[293]。ガス工作物の所有権の帰属を問わないことが示唆されている点で[294]、器物損壊罪とは制度趣旨を異にする。

損壊も機能障害行為もいずれも、供給妨害の原因行為である必要がある[295]。

損壊の解釈として、電気事業法のときの説明と類似して、損壊とは「広義の毀棄の一種であって、物の実質または効用を侵害する行為をいい、一部を損壊するをもって足り、必ずしもその破損のためにガス工作物の効用を全く不能ならしむることその破損部分がガス工作物の主要部分たることを要しない」と説明される[296]。しかし、機能の障害におい

---

[291] 【旧瓦斯事業法22条】遠藤・前掲注[242]391頁。
通商産業省公益事業局ガス課『ガス事業法』167頁(日本瓦斯協会、1954)は、1項及び2項の行為について、行為その者が社会公共上の安全に重大な支障を及ぼすと述べる。

[292] 経済産業省『ガス事業法の解説』315頁(ぎょうせい、2004)。

[293] 通商産業省公益事業局ガス課『ガス事業法』165頁、経済産業省・前掲注[292]316頁。

[294] 経済産業省・前掲注[292]316頁。

[295] 通商産業省公益事業局ガス課・前掲注[291]165頁。

[296] 通商産業省公益事業局ガス課・前掲注[291]166頁、経済産業省・前掲注[292]316頁。

て損壊に至らない範囲のガス工作物の本来の効用を発揮すべき能力の侵害が含まれると解されているのであるから[297]、損壊は物理的損壊のみを指し、機能の障害は、ガス工作物の本来の効用を害する行為と解すべきではないか、と考える[298]。機能障害の例は、LPGローリー車の燃料に異物を混入して運行を遅延させることによって、その効用を妨げる場合である[299]。

電気事業法115条の罪と同様に、ガスの供給妨害は現実に発生することが必要だと解される[300]。これは故意の内容でもある[301]。現実の供給妨害が発生しなかった場合には未遂犯の成立の余地があるにとどまる[302]。ここでいうガスの供給とは、使用者がガスを使用できる状態に置くことであり、供給に関係ある範囲においてガスの発生設備から使用者のガス栓までを含む[303]。

第２目　２項ガス供給妨害罪

本罪は、ガス工作物をみだりに操作して、ガスの供給を妨害することで成立する。「操作」とはガス工作物本来の作動方法に従ってその機器を運用することである[304]。それゆえ、「みだりに」の要件で処罰範囲を限定しなければならないことになる。電気事業法の解釈でも述べたとおり（第１款第２項第２目(2)）、原則としての不操作義務を肯定することによって、こうした包括的な処罰を可能にする条文の説明を行う必要があると思われる。

---

(297)　通商産業省公益事業局ガス課・前掲注(291)166頁。例として送炭機用レールに砂等を投入して運航を遅延せしめて効用を害する行為が挙げられている。

(298)　前掲注(279)参照。

(299)　経済産業省・前掲注(292)316頁。

(300)　【旧瓦斯事業法22条】水越到和『瓦斯事業法概論』167頁（永全社、1930）。経済産業省・前掲注(292)316頁の説明はやや明瞭さを欠くきらいがあるが、本文の解釈と矛盾はしない。

(301)　【旧瓦斯事業法22条】水越・前掲注(300)167頁。

(302)　経済産業省・前掲注(292)316頁。

(303)　経済産業省・前掲注(292)316頁。

(304)　通商産業省公益事業局ガス課・前掲注(291)166頁。

本罪の主体は問わないところ、ガス事業従事者でない一般人については、操作権限を肯定できないとして可罰的だという帰結を導きやすいが、ガス事業従事者にとっては一定の権限に基づいた操作権限を持つことがある以上、解釈を明確にする必要がある。ガス事業従事者については、そのガス工作物の操作の任にあらざる者またはその操作の任にある者であっても正常な職務上の操作にあらざる場合のガス工作物の操作が「みだりに操作」にあたるとされる(305)。形式的に一定の権限を持つ者による職務上の操作としての正常性が本罪の解釈上の課題となってくる。

第２項　ガス工作物施設変更罪

ガス工作物施設変更罪の主体は問わない(一般人でもガス事業従事者でもよい(306))(307)。ガス工作物の保安について、所有権の如何を問わず売渡内管といえども、全てガス事業者が保安の責任を負うから、その前提でガス工作物の変更を自由に放任してしまうとガス事業者に酷になるばかりでなく、粗悪な変更工事によるガスの漏えい等公共の安全を害する結果となるからである(308)。つまり、本罪も公共危険犯と捉えられている(309)。

ガス工作物の「変更」とは、移転、変換はもちろん、損壊しない範囲内における損傷及び加工設備をなすことを包括している(310)。増設も含む(311)。導管の取替えや押しつぶしはもちろん、メーターの逆転等が変更にあたる(312)。

---

(305)　通商産業省公益事業局ガス課・前掲注(291)166頁。

(306)　ただし、ガス事業従事者が職務上包括的に委任された範囲内において行う変更については「ガス事業者の承諾を得ないで」の要件を充たさないので犯罪は成立しない(通商産業省公益事業局ガス課・前掲注(291)168頁(1954)参照)。

(307)　通商産業省公益事業局ガス課・前掲注(291)168頁。

(308)　通商産業省公益事業局ガス課・前掲注(291)168頁。

(309)　【旧瓦斯事業法22条】水越・前掲注(300)167頁。

(310)　通商産業省公益事業局ガス課・前掲注(291)168頁。

(311)　【旧瓦斯事業法22条】水越・前掲注(300)167頁。

(312)　通商産業省公益事業局ガス課・前掲注(291)168頁。

緊急措置の場合は本条に該当しない、と解説されているが[313]、緊急措置には緊急避難や推定的同意等の場合が考えられるところ、これらはそもそも違法性阻却事由である。それゆえ、もし、「本条に該当しない」と解したい場合、「みだりに」を単に違法性阻却の不存在を要件化したものだと読む必要がある。

第３款　水道インフラの保護

水道インフラの保護は、刑法上の飲料水に対する罪と水道法51条の罪の双方によって規制されている。水道の供給に対して攻撃を加える場合は刑法147条及び水道法51条が、飲料の清浄性に対する侵害[314]については、刑法142条から146条の罪が問題となるので、この順に検討していく。

第１項　水道の供給に対する攻撃

水道損壊・閉塞罪は、１年以上10年以下の重い法定刑を有しており、また水道法51条の罪も最高刑は５年と比較的重い刑罰規定となっている。処罰範囲は水道法51条の罪の方が広く、刑法で処罰できない部分を、水道法で処罰しているともいえる[315]。

第１目　水道損壊・閉塞罪

本罪の罪質については争いがある。本罪を公共危険犯ではなく、水道の利用妨害だと解する説もある[316]。もっとも、多数説は、水道の供給の妨害により、公衆の生命・健康に危険が生じるので公共危険犯だとする[317]（保護法益は公衆の衛生[318]）。ここでは、水道に依存する公衆の健康

313　通商産業省公益事業局ガス課・前掲注(291)168頁。

314　さらに、水質汚濁防止法等も問題となる。

315　団藤・前掲注(60)243頁。

316　山口・前掲注(70)418頁、山中・前掲注(70)571頁、浅田ほか・前掲注(87)314頁〔金尚均〕、西田〔橋爪補訂〕・前掲注(67)346頁。ほかに、健康危険罪であることを認めつつも、直接的には水利妨害の側面の方が強いという指摘や小暮得雄編『刑法講義各論』407頁〔村井俊邦〕（有斐閣、1988）、水利妨害の要素もあり、水道汚染罪に法定刑が類似している、という指摘に『大コンメンタール 第３版 第７巻』429頁〔古江頼隆〕。

317　『大コンメンタール 第３版 第７巻』429頁〔古江頼隆〕。

に対する抽象的危険（渇水の危険）が問題になっているといえる[319]。本罪の刑が重いのはこうした公衆衛生に危害が及ぼす点に求められるとも指摘される[320]。未遂犯は不可罰であるが、処罰すべきだという批判もある[321]。

（1） 行為客体としての公衆の飲料に供する浄水の水道

水道とは、飲料水の輸送のために特設した水路のことをいい、浄水施設、濾過施設、その他鉄管、鉛管等、一切の機関が含まれる[322]。その所有権者、及び設備費用の拠出者には依存しない[323]。

（2） 行為としての損壊または閉塞

損壊とは物理的毀損のことをいう[324]（破壊[325]とされることもあるが破壊とは何かが問題となろう）。部分品の抜き取りもこれに含まれる[326]。閉塞とは有形の障害物により水流を塞ぐことだと解される[327]。一部の断絶か絶対的な断絶かを問わない[328]。損壊または閉塞の概念の中に入れて考えることもできるが、本罪の罪質に照らし、最終的に浄水の供給を不

⑶⑴⑻ 滝川春雄＝竹内正『刑法各論講義』332頁（有斐閣、1965）。

⑶⑴⑼ 西田典之＝山口厚＝佐伯仁志『注釈刑法　第２巻』349頁〔深町晋也〕（有斐閣、2016）（以下『注釈刑法 第２巻』として引用）。

⑶⑵⑽ 泉二新熊『日本刑法論 下巻（各論）訂44版』220頁（有斐閣、1939）。刑法147条も含めて、飲料水に対する罪を公衆衛生の見地から人の健康を保持するために設けられたものとする裁判例に福岡高判昭和26年12月12日刑集４巻14号2092頁。

⑶⑵⑴ 植松正『再訂 刑法概論Ⅱ各論』194頁（勁草書房、1975）。植松は水道法が処罰範囲の不足部分を補っているというが、電気事業法及びガス事業法上の罪と異なり、後述する水道法51条の罪は未遂犯を処罰していない点には注意を要する。

⑶⑵⑵ 大場茂馬『刑法各論』196頁（日本大学、1910）。

⑶⑵⑶ 岡田庄作『刑法言論 各論』253頁（明治大学出版部、1924）。

⑶⑵⑷ 松原・前掲注⑹⓪439頁、浅田・前掲注⑺⓪386頁、滝川＝竹内・前掲注⑶⑴⑻335頁。

⑶⑵⑸ 大谷・前掲注⑺④430頁。

⑶⑵⑹ 滝川＝竹内・前掲注⑶⑴⑻335頁。

⑶⑵⑺ 滝川ほか・前掲注⑶⑵⑹335頁。

⑶⑵⑻ 大谷・前掲注⑺④430頁。

能または著しく困難にすることが必要だとするのが多数説である(329)。水道施設自体の操作により送水を遮断することは含まない(→水道法51条２項)(330)。

(3)　サイバー攻撃への対応可能性

既に往来妨害罪(刑法124条)のところで述べたところと同様、本罪は、物理的な損壊または閉塞のみを捕捉する。もちろん、サイバー攻撃に基づいて物理的な損壊または閉塞を惹起させることはできるかもしれないが、サイバー攻撃それ自体を行為態様に含めることができない点で不足があるともいえる。一方で、水道法51条の罪は、刑法147条よりも行為態様の捕捉範囲が広いので同罪をみていきたい。

第２目　水道法51条の罪

水道法51条に水道の安定供給を担保するための罰則がある。

> 水道法第51条１項　水道施設を損壊し、その他水道施設の機能に障害を与えて水の供給を妨害した者は、５年以下の懲役又は100万円以下の罰金に処する。
> ２項　みだりに水道施設を操作して水の供給を妨害した者は、２年以下の懲役又は50万円以下の罰金に処する。

(329)　山口・前掲注(70)418頁、中森・前掲注(125)204頁、西田〔橋爪補訂〕・前掲注(67)348頁、浅田・前掲注(70)386頁、小暮得雄編『刑法講義各論』407頁−408頁〔村井俊邦〕(有斐閣、1988)。

大阪高判昭和41年６月18日判時472号66頁。

他の表現をする学説もあり、例えば団藤重光編・前掲注(137)284頁〔小暮得雄〕は「水道上水の供給を不可能にする程度にいたること」としてかなり厳しい要件を要求し、一方で大阪高判昭和49年６月12日刑集29巻７号431頁は「水道による浄水の供給を不可能または困難にする程度に破壊を加えること」として「著しく」を除いた表現をするが、実際上の差異が明らかではなく、その検討も困難であり、また本稿の目的とやや離れることから、本稿ではこれ以上踏み込まないことにする(学説の対立については『注釈刑法　第２巻』351頁〔深町晋也〕、『大コンメンタール 第３版 第７巻』432頁〔古江頼隆〕参照)。

(330)　大阪高判昭和41年６月18日判時472号66頁。

> ３項　前２項の規定にあたる行為が、刑法の罪に触れるときは、その行為者は、同法の罪と比較して、重きに従って処断する。

法51条の罪は侵害犯と解されており、水の供給を遮断する等して現実に妨害した事実の発生が必要である[331]。電気及びガス事業法の場合と異なり、未遂犯は処罰されない。行為者は問わない（一般人も水道関係者も本条の罪を犯し得る）[332]。

同時に、本罪は業務妨害罪的な規定だと解されている[333]。ただし、刑法上の業務妨害罪は抽象的危険犯であるから、その捕捉範囲が異なり得る。本罪が成立する場合には業務妨害罪とは法条競合（特別関係）になるだろうが、業務妨害罪だけ成立する段階において同罪の成立を否定する理由はないだろう。事実上、業務妨害罪が本罪の未遂処罰の機能を担っている。

また、水道法51条の罪が水道事業の保護も考慮しているという前提を採ると、本罪と水道損壊・閉塞罪とは観念的競合になる[334]。３項はこの点を確認したものだとされる。法条競合の特別関係になるわけではない、という意味では同項の存在に意味を見いだせよう。

(1)　行為客体としての「水道施設」

水道施設は、法３条８項において、「水道のための取水施設、貯水施設、導水施設、浄水施設、送水施設及び配水施設（専用水道にあっては、給水の施設を含むものとし、建築物に設けられたものを除く。以下同じ。）であって、当該水道事業者、水道用水供給事業者又は専用水道の設置者の管理に属するもの」と定義される。

問題となる水道のための施設を特定した上で、水道事業者等にそれに

---

[331]　日本水道協会『水道法逐条解説　第４版』702頁−703頁（2015）。

[332]　日本水道協会・前掲注[331]703頁。

[333]　奥村誠「公衆の健康に関する罪（その一）」ジュリ463号136頁、138頁（1970）。

[334]　『大コンメンタール　第３版　第７巻』434頁〔古江頼隆〕。もっとも、西田〔橋爪補訂〕・前掲注[67]348頁は、水道損壊罪の特別法に水道法51条の罪があるというが、仮にそう解釈できたとしても、水道法51条３項の規定により観念的競合としての処理をすべきだと考えられる。

対する管理権があるかどうかを吟味し、これがある場合に限り、本法における水道施設にあたる。例えば、水道事業者が当該ダムの管理権を有しない貯水池から取水している場合には、その貯水池は、水道施設ではないが、一方で、水道用の貯水池が他の用途との共用のものであっても、その管理権を水道事業者(共同の管理権であっても差し支えない。)が有する場合には、水道施設だとされる(335)。

(2)　1項供給妨害罪

「損壊」とは、機能障害の例示であって(336)、物の実質又は効用を侵害する行為をいい、一部の破損をもって足り、必ずしも水道施設の効用を全く不能ならしめる程度の破損であることは必要としない、とされているが(337)、電気及びガス事業法の部分で既に述べたとおり、機能障害も捕捉されているのだから、ここでいう損壊は物理的損壊に限るべきである。破損部分が水道施設の主要部分である必要はない。

「機能に障害を与え」とは、損壊に至らないが水道施設の本来の能力に支障を及ぼすことをいう(338)。例えば、修復が可能か否かを問わず、導水、送水、配水等の導管を土石等でつまらせ、ポンプ、モーター等の機械類のネジをゆるめ、又は取り外す等して正常な運転を不能ならしめる場合がこれにあたる(339)。

「水の供給の妨害」には、供給を全く不可能にする場合、及び供給を困難にする場合があたる(340)。単に危険があるだけでは足りない(341)、とされているから、侵害犯だと解されている。故意の内容でもある(342)。

(3)　2項供給妨害罪

1項と同様、水の供給の妨害という結果が発生することを必要とする

---

(335)　日本水道協会・前掲注(331)106頁。
(336)　安西・前掲注(218)163頁。
(337)　日本水道協会・前掲注(331)703頁。
(338)　日本水道協会・前掲注(331)703頁。
(339)　日本水道協会・前掲注(331)703頁。
(340)　安西・前掲注(218)163頁。
(341)　日本水道協会・前掲注(331)703頁。
(342)　安西・前掲注(218)163頁。

侵害犯だと解される(343)。２項供給妨害罪について水の供給の妨害の認識を不要とする説もあるが(344)、侵害犯説に立つ場合、理由がないように思われる。

「みだりに」とは、正当な理由がなくという意味であって、操作の日的、方法が法規に違反する場合は勿論、公序良俗、条理に反する場合が含まれる(345)。

操作とは、水道施設本来の作動方法に従って運転ないし運用することをいう(346)。

水道制水弁の操作による送水の遮断は本罪に該当する(347)。水道施設の操作によって送水を遮断することは水道の閉塞にあたらないゆえに、本罪で捕捉するほかない(大阪高判昭49年６月12日〔この事案では損壊が認められた〕)。

第２項　水の清浄性に対する侵害

サイバー攻撃によってCPSとして機能する飲料水の消毒システム等がハッキングされ、その結果塩素等の消毒薬が過剰に飲料水に混入したり、あるいは消毒薬の投入が停止して飲料用の水の中の細菌が増えたりすることが考えられる。そうした状況の発生に気づかずに飲料水を供給してしまったり、そうした状況の発生によって飲料水を供給できなった

	を汚染し、よって使用することができないようにした	毒物その他人の健康を害すべき物を混入した
人の飲料に供する浄水	142条	144条
水道により公衆に供給する飲料の浄水又はその水源	143条	146条

(343)　日本水道協会・前掲注(331)703頁は、そのように解していると読める。
(344)　安西・前掲注(218)163頁。
(345)　日本水道協会・前掲注(331)703頁。
(346)　日本水道協会・前掲注(331)703頁。
(347)　大阪高判昭和41年６月18日判時472号66頁。

りするおそれがある。刑法は142条以下のいくつかの規定で飲料水等をその汚染等から保護している。

第１目　罪質・保護法益

汚染に関する罪(142条、143条)については、客体により法定刑の差が大きく、その保護法益の内容について一定の争いがある。公衆の健康というように保護法益を捉えるのが一般的ではある(348)。しかし、水を飲んで健康を害することについての危険なのか、水を飲めなくなることについての危険なのか(渇水の危険)、という対立軸もあり得るし(349)、原則的に公共危険犯と捉えると不特定又は多数人の保護という議論がついて回るが、そもそも刑法142条、144条の罪については、問題となっているのは公衆ではなく人であるから、特定かつ少数の人の健康も保護していると解すべきである、という指摘もなされている(最近の有力説である。元々存在した「不特定又は多数」という定式に対して共有している疑問を素直に定式化した説だともいえる)(350)。

第２目　行為態様のサイバー攻撃対応可能性

次に、行為態様にサイバー攻撃を含めることができるだろうか。刑法142条、143条については、客体を「汚染し、よって使用することができ

---

(348)　大判昭和８年６月５日刑集12巻736頁は「飲料水ニ關スル罪ナルモノハ公共衞生ノ見地ニ於テ人ノ健康ヲ保持スル爲設ケラレタル罰則」だとする。

(349)　『注釈刑法 第２巻』334頁-335頁〔深町晋也〕。

(350)　特定かつ少数でもよいとする説に『注釈刑法 第２巻』336頁-337頁〔深町晋也〕。

もっとも、刑法142条、144条も含めて、大判昭和８年６月５日刑集12巻736頁を始め、不特定又は多数人を保護していると解する学説が通説的である。例えば、『大コンメンタール 第３版 第７巻』408頁以下〔古江頼隆〕、山口・前掲注(70)416頁、中森・前掲注(125)202頁、松原・前掲注(60)437頁、大竹武七郎『刑法綱要 総論各論』374頁(1935)。

西田〔橋爪補訂〕・前掲注(67)346頁も本罪の公共危険犯性を理由として同じ考えを採る。さらに松原・前掲注(60)437頁、浅田・前掲注(70)382頁、団藤・前掲注(60)239頁。判例によれば「特定人ニ對シ飲用セシムル目的ヲ以テ茶椀等ニ淨水ヲ盛リタル場合」は除かれる(大判昭和８年６月５日刑集12巻736頁)。

ないようにした」という文言の解釈が問題となる。汚染→使用不能という因果過程を分けて考えるか(結果的責任、使用不能の認識も不要になる)[351]、飲用できない程度に汚染することをいうのか(この場合、使用不能になることの認識を要する)[352]、争いがある[353]。使用不能とは、飲料水として使用できないことをいい、物理的又は心理的に使えない(飲用をためらう[354])状態のことをいう[355]。もっとも、汚染それ自体は水を不潔にする一切の行為であって方法の如何を問わない[356]。それゆえ、サイ

西田〔橋爪補訂〕・前掲注(67)346頁、山中・前掲注(70)568頁、大谷・前掲注(74)427頁、団藤・前掲注(60)239頁、団藤重光編・前掲注(137)275頁〔小暮得雄〕は、不特定又は多数人説を採用するが、143条との関係で「ある程度の多数」(数人でもよい)でよいとする。ただし、「ある程度」の線引きが解釈上の課題になる。この点で、青柳文雄『刑法通論 第2 各論』193頁(泉文堂、1963)は、不特定又は多数人説を採用しつつも、一個人(特定かつ少数人)が反復継続して使用する水瓶を来客が飲用する可能性がある場合には、刑法142条の対象になるとし、また、植松・前掲注(321)191頁は、反復利用する場合の特定少数を含むとしていた(こうした場合は不特定と考えてよいとするものに『大コンメンタール 第3版 第7巻』409頁-410頁〔古江頼隆〕)。結局のところ、『注釈刑法 第2巻』337頁〔深町晋也〕のいう「人」の解釈として特定かつ少数で足りる、とするのが、法定刑や文言の相違を踏まえても、明解な解釈だと思われる。

(351) 泉二・前掲注(320)218頁-219頁、大竹・前掲注(350)374頁。

(352) 山口・前掲注(70)416頁、中森・前掲注(125)202頁、松原・前掲注(60)438頁、浅田・前掲注(70)383頁。「よって」は結果的加重犯であることを示したものではない、とする。山中・前掲注(70)568頁-569頁、青柳・前掲注(350)193頁〔使用不能とは汚した程度を示す概念である〕。

(353) 争いの状況についてより詳しくは『大コンメンタール 第3版 第7巻』412頁〔古江頼隆〕、団藤重光編・前掲注(137)276頁〔小暮得雄〕。

(354) 青柳・前掲注(350)193頁。

(355) 山口・前掲注(70)416頁、中森・前掲注(125)202頁、松原・前掲注(60)438頁、浅田ほか・前掲注(87)312頁〔金尚均〕。

人の飲料に供する井戸水の中に食用紅を溶かした水を注ぎ込み、一見して異物の混入したことを認識し得る程度に薄赤色に混濁させ、飲料浄水として一般に使用することを心理的に不能ならしめる場合に刑法142条に該当するとした判例として最判昭和36年9月8日刑集15巻8号1309頁。

バー攻撃によって水を不潔にすれば、汚染といってよいだろう。もっとも、本罪はサイバー攻撃を想定して作られたものではないから、想定される行為類型はフィジカルなそれである。例えば、水を清潔に保つための消毒薬の制御システムをハッキングしてその機能を停止させる行為それ自体は、それによって汚染状態が発生するまで、汚染とは呼べない。本罪は未遂犯を処罰しないから、水の汚染を目的としたハッキング自体を捕捉することは、現行法上は難しいように思われ、立法論的な課題が残る。

刑法144条については「毒物その他人の健康を害すべき物を混入した」という文言の解釈が問題となるが、混入とは、混じって容易に分離し得ない状態の作出であり(357)、これがフィジカル面の状態の変更を意味することは明らかである。それゆえ、上記の汚染と同様に、(想定しがたいかもしれないが)混入目的のハッキングそれ自体を捕捉することが難しい。

第３目　検討

飲料水に関する罪については、「公衆」の健康を保護するか否か、言い換えれば、悪影響の範囲の程度によって、法定刑が異なる規定が使われている点に特徴がある。CPSを保護する際に、広範囲の社会的な悪影響が生じる場合のみを刑法で保護すべきであるというのであれば、刑法143条、146条の罪で問題となる客体のハッキングを捕捉すべきである、という議論も可能かもしれず、他の国の議論も見ながら検討していくべきである。

第３節　小括・インフラの保護

第１款　インフラ保護のための刑事立法の特徴

交通インフラと電気・ガス・水道インフラの保護について簡潔にみてきた。特徴的な部分に絞ってみると、我が国の特別法上の上記のインフラ保護は供給妨害罪を利用してなされており、１項犯罪としての機能障害に基づく罪(新幹線特例法２条、電気事業法115条、ガス事業法192条、水道法51条)と、２項犯罪としてのみだりに操作罪を持つ類型が複数ある

(356)　『大コンメンタール　第３版　第７巻』410頁〔古江頼隆〕。
(357)　『大コンメンタール　第３版　第７巻』419頁〔古江頼隆〕。

ことがわかる。２項の操作の概念は本来の作動方法に従ってその機器を運用することであり、２項の行為が直ちに１項の損壊や機能障害を惹起するわけではなく、１項と２項の処罰範囲は互いに完全に重なり合うわけではない。

サイバー攻撃の場合にも、１項に該当することはあり得るかもしれないが、サイバー攻撃の性質上、システムの物理面というよりはその制御に対する無権限の干渉が可能になっているから、１項よりもむしろ２項のみだりに操作罪が成立することが多いと思われる。もっとも、みだりに操作罪は物理的な操作を念頭において作られたと推測されるから、サイバー攻撃に対応させるためにはより議論を精緻化させる必要があるようにも思われる。例えば、外部者の攻撃であれば、不正な指令を送った時点等、外形的に行為を特定しやすいと思われる一方で、内部者によるみだりに操作の場合に、権限のない処理をさせる意図でシステムの使用を開始した時点等、行為の特定が曖昧になりやすい嫌いがある。すなわち、解釈論としては「操作」の概念の精緻化が、立法論としては「操作」に代わる文言を考える必要があり得る（この文脈では解釈論と立法論が類似してこよう）。さらに法定刑の適切性の問題もあり得る。行為の特定問題を含むこうした課題を、比較法的な検討を行う際に念頭に置いておくべきである。

第２款　俯瞰的に見た我が国の刑事法によるインフラ保護

より俯瞰的にみると、まず、法技術的に、我が国では、その具体性には幅がありうるが、具体的なインフラ毎に、その整備のために特別法を用いて規制し、それに付随する形で罰則を設けることでその安全を図ろうとしている。

次に、刑法理論的に見ると、我が国では、重要インフラの保護については、公共危険犯と業務妨害罪的犯罪の組合せにより保護が行われてきていることを指摘できる[358]。刑事立法の文脈でも業務妨害罪のみがある状況では足りないので公共危険犯を設けるべきだという議論がなされ

[358] 移動体（航空機）を財産犯的規定で加重処罰する運航支配罪は例外的であった。

ていた(359)。もっとも、サイバー犯罪対策立法の文脈では、業務妨害罪を加重したものの(刑法234条の２)、公共危険犯に対しては直接手が入ることはなかった。

そこで、電子計算機損壊等業務妨害罪に公共危険犯的要素を加えた加重立法を行うべきなのか、あるいはサイバー攻撃的な要素を要件とする加重された公共危険犯を考えていくべきなのか、どのようなアプローチがよいのか、が課題となって残る。

フィジカルインフラの保護の文脈では、公共の危険を惹起しうるサイバー攻撃に対してどのようにアプローチするかが問題となっているので、この点について、国際的な法状況を知る必要がある。

本研究はJSPS科研費20K13356の助成を受けたものです。

(359)　飲料水に対する罪についての刑法改正の議論について奥村・前掲注(333)138頁。