

令和 6 年 4 月 10 日現在

機関番号：12501

研究種目：若手研究

研究期間：2020～2023

課題番号：20K13356

研究課題名（和文）サイバー・フィジカル・セキュリティの維持・向上のための刑法的規制

研究課題名（英文）Criminal regulations for maintaining and improving "cyber physical security"

研究代表者

西貝 吉晃（Nishigai, Yoshiaki）

千葉大学・大学院社会科学研究院・准教授

研究者番号：50707776

交付決定額（研究期間全体）：（直接経費） 4,700,000円

研究成果の概要（和文）：サイバー攻撃によって物理空間への害を発生させることがある。こうしたサイバー攻撃に対する適切な処罰の在り方を模索したのが本研究である。

特別法を含む既存の罰則群を調査し、サイバーフィジカルセキュリティの保護が十分かどうかを検証した。その結果、我が国には多くの処罰規定が存在するが、サイバーフィジカルセキュリティとの関係で、十分な処罰が可能であるとは断言できない法状態であることがわかった。

そこで、ドイツ刑法などの議論を参照し、サイバーフィジカルセキュリティの保護に対応する犯罪類型についての調査・研究を行い、この比較法的知見を我が国の刑法上の議論に応用する立法論を展開した。

研究成果の学術的意義や社会的意義

本研究は、最近、活発に行われている刑事立法学の研究の一つを示す。本研究は、解釈の限界を認識した上で、よい規定の作り方という意味では伝統的な立法論かもしれないが、刑事立法学が比較的新しい研究分野であることに照らすと、各論的検討として学術的な意義がある。

また、サイバーフィジカルセキュリティの維持は、現在においては、重要インフラの保護等の観点から、国家的な問題関心だといえる。これについて、政策的な議論が政府によっても随時進められているが、我が国においては刑事立法の議論は盛んではない。本研究は現実の立法論の準備作業という位置付けを与えることができ、この点に重要な社会的意義を見いだすことができる。

研究成果の概要（英文）：Cyber attacks can cause harm to physical space. This study sought to find appropriate criminal penalties for such cyber-attacks.

A survey of existing criminal penalties, including special laws, was conducted to determine whether these laws are sufficient for the protection of cyber-physical security. As a result, it was found that although there are many penalties in Japan, the current state of the law does not assure adequate punishment in relation to cyber-physical security.

Therefore, referring to discussions in the German Criminal Code and other criminal laws, research was conducted on the types of crimes corresponding to the protection of cyber-physical security, and a legislative theory was developed to apply this comparative legal insight to discussions in the Japanese Criminal Code.

研究分野：刑法

キーワード：サイバーフィジカルセキュリティ サイバーセキュリティ 刑法 不正指令電磁的記録 電子計算機損壊等業務妨害罪 IoT 刑事立法学

1. 研究開始当初の背景

サイバー・フィジカル・セキュリティは、研究期間中、例えば「重要インフラ」の保護、という文脈で、その重要性が謳われてきているものである。

研究開始当初においても、外国においては、サイバーテロの抑止などの文脈で特別な処罰規定が置かれたり、処罰の議論こそ行われていないが、我が国においても、経済産業省などにおいて、サイバー・フィジカル・セキュリティの保護に関連するガイドラインなどが作られたりするなどしていた。そのため、研究開始の時点(2020年4月)から、研究が終了した現在(2024年4月)に至るまで、その重要性は失われていない。それどころか、情報通信技術(ICT)のますますの発展に伴い、本研究の議論の重要性はより増したともいえる。もっとも、外国と異なり、処罰規定を強化すべきではないか、といった議論が我が国のサイバー・フィジカル・セキュリティの文脈では必ずしも活性化していなかった。そうした状況が、本研究の開始のきっかけであった。

2. 研究の目的

上記のような背景事情を受け、本研究においては、サイバー・フィジカル・セキュリティを罰則によってどのように確保するか、を検討することを目的とした。サイバー・フィジカル・セキュリティの侵害は、サイバー空間でその影響が閉じる従来のサイバー犯罪と異なり、人の死傷やインフラの停止などを伴い得る重大な事件だといえる。にもかかわらず、そうした事件を起こした犯人を重い犯罪で処罰しようとする場合において、フィジカル面への侵害を想定しないで作られた、相対的には軽い刑しか有しない犯罪類型しか用意されていない、というのでは、法状態としては不十分だと評価されかねない。そこで、サイバー・フィジカル・セキュリティの侵害に関連する犯罪類型を調査しつつ、その不十分さがあればそれを指摘し、サイバー・フィジカル・セキュリティの保護に資するような犯罪類型を新しく作る必要がある場合にはそれを提案することを目的として研究を進めた。

3. 研究の方法

(1) サイバー・フィジカル・セキュリティの政策論と現行法

研究の方法としては、本研究の目的であるサイバー・フィジカル・セキュリティに関する政策論を調査した上で、これに関する国内の処罰規定の解釈論を確認した。こうした処罰規定の中には、サイバー犯罪対策規定もあれば、放火罪や飲料水に関する罪等の公共危険犯と呼ばれるものもある。サイバー犯罪対策規定では、人の死亡まで考慮していない一方で、公共危険犯は「サイバー」に関する行為を考慮しておらず、どっちつかずの状況があるように思われたので、さらに特別法上の犯罪(みだりに機器を操作する罪など)にも調査対象を拡げて検討を行った。

(2) サイバー犯罪対策規定の解釈論

同時に、マルウェア関連犯罪や電子計算機損壊等業務妨害罪といったサイバー犯罪対策規定じたいを深く検討した。2つの犯罪の選択は、サーバのダウンなどに繋がる行為を規制していると考えられ、発散しがちな検討対象をよく限定しようとする試みでもあった。マルウェア関連犯罪については、研究期間中に重要な先例となるコインハイブ事件最高裁判決(最判令和4年1月20日刑集76巻1号1頁)が出たため、これの検討も行うこととし、電子計算機損壊等業務妨害罪はインフラ保護と密接に関係するという理解から、網羅的な調査を行った。

(3) 比較法

さらに、ドイツ、オーストリア、イギリスなどの国におけるサイバー・フィジカル・セキュリティの保護に関係すると思われる規定についての立法論及び解釈論を調査した。とりわけ、ドイツ刑法については、303条a、303条bという、同国においては比較的よく使われるが、我が国においては完全に対応する規定を見つけづらい(あるいは、対応する規定はあるのだが、あまり使われていない)規定について、その立法から解釈・運用に至るまでの網羅的な調査を行った。EU圏の国々においては、EU指令によって、立法が促されることがあるので、必要に応じてEU指令に関する議論の調査もした。外国法の調査は、木を見て森を見ず、にならないように、時間の許す限りで網羅性を心がけた。

(4) 知見の融合

(1)~(3)で得た知見を融合させて、サイバー・フィジカル・セキュリティの維持・向上を実現する刑法的な規制の在り方を検討した。

4. 研究成果

3. で述べた方法を採用することにより、比較法的な観点(3.(3))からは、ドイツやオーストリア等の国においては、サイバー空間内の害しかもたらさない場合を主に想定するサイバー犯罪対策規定だけでなく、フィジカル空間にも害を及ぼす場合により重く処罰する規定をもっていることがわかった(西貝吉晃「コンピュータ・サボタージュ罪刑法303条b ドイツ刑法典の改正(2)」刑事法ジャーナル71号(2022)97-114頁、西貝吉晃「データ変更罪—刑法303条aの創設とその運用: ドイツ刑法典の改正(7)」78号(2023)112-155頁)。一方で、3.(1)の調査結果(西貝吉晃「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」千葉大学法学論集36巻1号(2021)160-58頁)からは、我が国はそうした規定を有していないことがわかった。もっとも、当時の新しい技術(例えば新幹線も含む)に対して、特に刑法的保護を提供しようとする法律が作られるなどはしており、現在のICT技術の革新に対しても、同様の立法論を展開すべきではないか、という考察の契機を得ることができた。

フィジカル空間をも適切に保護するためにサイバー犯罪対策規定を加重して対応しようという立法姿勢は、IoT時代において、フィジカル空間を守るためにも情報通信を行う機器のセキュリティが重要視されていることにも鑑み、我が国の法律論としても是認され得るものだと考えた。もっとも、抽象的に加重処罰規定を置くという議論をするだけでは足りず、立法論として、どのような処罰規定が適切か、という議論をしないと先には進めない。

そこで、3.(2)で述べた国内のサイバー犯罪対策規定のどの規定を出発点として議論を進めるべきかを考えることとなった。マルウェアなどのツールによらないで、大規模な損害を発生させることが可能である以上、ツールの存在を前提とし、かつツールの使用により発生する実害にあまり意を払っていない不正指令電磁的記録に関する罪に着目するのではなく、電子計算機損壊等業務妨害罪が妥当であるという理解に達した。

その上で、電子計算機損壊等業務妨害罪を思考のベースラインとして考えつつ、複数の国の法律論を検討した。結果として、セキュリティ侵害行為によって、重大な結果を惹き起こし得るシステム内の一部分に侵入し、そこでのシステムの挙動を決定するデータに対するアクセスを得ることに危険性を見いだせる、という理解に基づき、他国法から得た法的知見を参照することにより、いくつかの立法論の道筋を得た。そして、保護すべきインフラをある程度特定し、それを客体とするサイバー犯罪対策規定の特別な加重処罰規定を置くという方法が適切ではないか、という結論を得た。保護すべきインフラの規定上の特定方法についてなお課題はあるものの、現時点では、我が国において立法論が盛んなわけではないため、将来的に問題になったときに有益だといえる程度に、現行の法律などと比較しながら、アイデアを得るにとどまった。得た知見については、単著論文として近日中に刊行される予定である(2024年4月時点)。

こうした議論をする際に、我が国のサイバー犯罪対策規定の解釈論やドイツ刑法の紹介について、詳細な研究成果を複数得ることができたのは、本研究の遂行の際に得た重要な副産物である。例えば、マルウェアに係る不正指令電磁的記録に関する罪については、研究期間中にサイバー・フィジカル・セキュリティとは直接関係しない場合があることを認めつつ、第一義的には、本研究に直接結びつけはしないものの、本研究の目的との関係に目を配りつつ、コインハイブ事件最高裁判決に対する評釈、不正指令電磁的記録に関する罪の解釈論、及びマルウェア関連犯罪に関する立法論(法改正の提案)などを提示することができた(西貝吉晃「技術と法の共進化を企図した法解釈の実践: コインハイブ高裁判決を素材に」法学セミナー792号(2021)40-46頁、同「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(2021)20-40頁、小田啓太=西貝吉晃「アプリ開発の実務を踏まえた不正指令電磁的記録に関する罪の一考察: コインハイブ事件を契機として」千葉大学法学論集36巻1号(2021)56-25頁、西貝吉晃「サイバーセキュリティの保護とイノベーションの促進の両立」法学セミナー808号(2022)46-55頁、西貝吉晃「罰則によるサイバー犯罪対策の課題: コインハイブ事件を契機として」ジュリスト1573号(2022)113-118頁、西貝吉晃「サイバーセキュリティと刑法—サイバー犯罪対策規定の解釈論と刑事立法学」佐伯仁志ほか編『刑事法の理論と実務』(2022)205-229頁、西貝吉晃「情報技術の発展と刑事立法及び刑法解釈—サイバー犯罪対策規定の動態的考察」有斐閣Online YOLJ-L2212004(2023))。また、電子計算機損壊等業務妨害罪についても、処罰範囲の適切な限定という目的から、その危険犯としての罪質理解をより具体化して特定するなど(具体的危険犯説の採用) 解釈論の精緻化を行うことができた(西貝吉晃「現時における電子計算機損壊等業務妨害罪の解釈論」警察学論集77巻2号(2024)53-105頁)。

いずれにしても、サイバー・フィジカル・セキュリティの刑法的保護に向け、将来現実化するかもしれない立法論に備える形で、学術的な意義だけでなく、社会的な意義をも有する立法論の基礎を構築することができたのではないかと考えている。

5. 主な発表論文等

〔雑誌論文〕 計13件（うち査読付論文 0件 / うち国際共著 0件 / うちオープンアクセス 2件）

1. 著者名 西貝吉晃	4. 巻 67, 5
2. 論文標題 サイバーセキュリティの保護とイノベーションの促進の両立：コインハイブ事件最高裁判決を素材に[最 一小判令和4.1.20]	5. 発行年 2022年
3. 雑誌名 法学セミナー	6. 最初と最後の頁 46, 55
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 西貝吉晃	4. 巻 1573
2. 論文標題 罰則によるサイバー犯罪対策の課題：コインハイブ事件を契機として	5. 発行年 2022年
3. 雑誌名 ジュリスト	6. 最初と最後の頁 113, 118
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 西貝吉晃	4. 巻 960
2. 論文標題 サイバー空間の新技术はどこから犯罪になるのか	5. 発行年 2022年
3. 雑誌名 世界	6. 最初と最後の頁 226, 235
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 西貝吉晃	4. 巻 -
2. 論文標題 情報技術の発展と刑事立法及び刑法解釈～サイバー犯罪対策規定の動態的考察	5. 発行年 2023年
3. 雑誌名 有斐閣Online Y0LJ-L2212004	6. 最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 西貝吉晃	4. 巻 1
2. 論文標題 Van Buren v. United States, 593 U.S. ___, 141 S. Ct. 1648 (2021) 内部ポリ シーに違反するコンピュータ使用行為について, 18 U.S.C. § 1030 (a) (2) における無権限アクセス罪の無権限とはいえないとされた事例	5. 発行年 2022年
3. 雑誌名 アメリカ法	6. 最初と最後の頁 151-158
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 小田 啓太、西貝 吉晃	4. 巻 36
2. 論文標題 アプリ開発の実務を踏まえた不正指令電磁的記録に関する罪の一考察 : コインハイブ事件を契機として	5. 発行年 2021年
3. 雑誌名 千葉大学法学論集 = Chiba journal of law and politics	6. 最初と最後の頁 56 ~ 25
掲載論文のDOI (デジタルオブジェクト識別子) 10.20776/S09127208-36-1-P056	査読の有無 無
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 西貝 吉晃	4. 巻 36
2. 論文標題 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	5. 発行年 2021年
3. 雑誌名 千葉大学法学論集 = Chiba journal of law and politics	6. 最初と最後の頁 160 ~ 58
掲載論文のDOI (デジタルオブジェクト識別子) 10.20776/S09127208-36-1-P160	査読の有無 無
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 西貝吉晃	4. 巻 489
2. 論文標題 電磁的記録	5. 発行年 2021年
3. 雑誌名 法学教室	6. 最初と最後の頁 38 ~ 43
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 西貝吉晃	4. 巻 58
2. 論文標題 不正指令電磁的記録に関する罪の解釈論	5. 発行年 2021年
3. 雑誌名 罪と罰	6. 最初と最後の頁 20～40
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 西貝吉晃	4. 巻 71
2. 論文標題 コンピュータ・サボタージュ罪刑法303条 b ドイツ刑法典の改正(2)	5. 発行年 2022年
3. 雑誌名 刑事法ジャーナル	6. 最初と最後の頁 97
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 西貝吉晃	4. 巻 1153
2. 論文標題 令和2年著作権法改正の刑法的検討	5. 発行年 2020年
3. 雑誌名 法律時報	6. 最初と最後の頁 77-83
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 西貝吉晃	4. 巻 792
2. 論文標題 技術と法の共進化を企図した法解釈の実践 : コインハイブ高裁判決を素材に	5. 発行年 2020年
3. 雑誌名 法学セミナー	6. 最初と最後の頁 40-46
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 西貝吉晃	4. 巻 35
2. 論文標題 刑事判例研究(Number 209)ひそかに児童の姿態を電磁的記録に係る記録媒体に記録した者が当該電磁的記録を別の記録媒体に記録させて児童ポルノを製造する行為と児童ポルノ法7条5項の児童ポルノ製造罪の成否[最高裁令和元.11.12決定]	5. 発行年 2020年
3. 雑誌名 論究ジュリスト	6. 最初と最後の頁 226-231
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

〔学会発表〕 計1件(うち招待講演 1件/うち国際学会 0件)

1. 発表者名 西貝吉晃
2. 発表標題 サイバー・フィジカル・セキュリティの刑法的保護・序説
3. 学会等名 第29回日本刑法学会仙台部会(招待講演)
4. 発表年 2022年

〔図書〕 計3件

1. 著者名 鎮目 征樹、西貝 吉晃、北條 孝佳、荒木 泰貴、遠藤 聡太、蔦 大輔、津田 麻紀子	4. 発行年 2022年
2. 出版社 弘文堂	5. 総ページ数 344
3. 書名 情報刑法 サイバーセキュリティ関連犯罪	

1. 著者名 石井 徹哉	4. 発行年 2022年
2. 出版社 成文堂	5. 総ページ数 304
3. 書名 AI・ロボットと刑法	

1. 著者名 櫻庭 信之、行川 雄一郎、北條 孝佳	4. 発行年 2021年
2. 出版社 商事法務	5. 総ページ数 324
3. 書名 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	

〔産業財産権〕

〔その他〕

-

6. 研究組織

氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
---------------------------	-----------------------	----

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関
---------	---------