

令和 2 年 7 月 3 日現在

機関番号：32665

研究種目：若手研究(B)

研究期間：2017～2019

課題番号：17K13638

研究課題名（和文）サイバー犯罪の研究 - CIA犯罪を中心に -

研究課題名（英文）Research on Cyber Crimes focusing on CIA crimes

研究代表者

西貝 吉晃 (NISHIGAI, Yoshiaki)

日本大学・法学部・准教授

研究者番号：50707776

交付決定額（研究期間全体）：（直接経費） 3,200,000円

研究成果の概要（和文）：サイバーセキュリティの維持・向上のため、サイバーセキュリティまたは情報セキュリティの定義でもある機密性・完全性・可用性の各項目の刑法の観点からの保護の仕方を探った。まず、そもそも情報とは何か？、及び情報セキュリティと法律との関係を考えて上で、不正アクセス等への対処方法について、諸外国が採用する法制を調査しつつ、現行の刑事実体法の改正の必要性、及び改正の方法を、自身の見解としてまとめて論文として公表した。なお、サイバー攻撃によるフィジカルへの悪影響に対する規制に対する刑法的アプローチがなお課題として残っている。

研究成果の学術的意義や社会的意義

第一に、情報やデータといった多義的な用語について、記号論的、及び通信工学的な知見を活かしつつ、多層的に分析する三分法を提案した。これを用いることにより、議論の次元が明確になることが期待される。今後の情報保護に関する法制度を考える際の基礎を構築できたと考える。

第二に、サイバーセキュリティそれ自体（例えば機密性）を刑法上の保護法益と考えつつも、刑法の謙抑性の要請と両立する形での処罰範囲を必要十分に限定する立法案を提示できた。新たな攻撃手法が生まれやすいこの領域において、適切な処罰範囲を有する処罰規定を提示することには大きな社会的意義があると思われる。

研究成果の概要（英文）：In this research, for the purpose of maintaining and improving cyber security, I considered an optimized approach to protect confidentiality, integrity, and availability of information and data, which is also the definition of cyber or information security. Before legal discussion, I analyzed what information or data is also from the perspective of semiotics and information technology, and how we protect cyber security using both technological measures and criminal law, and then using the information in relating to other countries' cyber crime statutes and their interpretations, I proposed some reform plans of preexisting criminal statutes in Japan, mainly focusing on hacking (unauthorized access offences). However, a criminal law approach how to prevent physical harm from occurring by cyber attacks still remains as my future tasks.

研究分野：刑事法学

キーワード：サイバーセキュリティ サイバー犯罪 情報・データ 記号論・情報学 無権限アクセス・ハッキング クラッキング Society5.0 サイバー・フィジカル・セキュリティ

科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。

## 様式 C - 19、F - 19 - 1、Z - 19 (共通)

### 1. 研究開始当初の背景

コンピュータ技術の発展及び普及に伴って、万人がこれを利用する時代が既に到来していた。コンピュータの普及を推進することは国家の重要な政策目的であり続けてある(デジタル・ディバイドの解消問題)。しかし、コンピュータの利用によってコミュニケーションに対して多大な利便性がもたらされたのと同時に、これを利用した他人の権利・利益を侵害する悪質な行為、サイバーセキュリティを侵害するサイバー犯罪も発生するようになった。このような悪質な行為を抑止し、安全にコンピュータやネットワークを利用できる環境を整えること、すなわち、サイバーセキュリティ(情報セキュリティ)の維持は重要な政策課題であり、技術や教育だけでなく、法規制も含めて考察が必要である。

そして、とりわけ研究開始当初の時点では、日本年金機構へのハッキングに基づく情報漏洩に関する事件が記憶に新しいところであった等して、サイバー攻撃の激化に伴い、サイバー犯罪対策立法の諸規定を見直し、必要であれば立法論を提示すべき状況があった。と同時に、諸外国と比較すると、我が国のサイバー犯罪対策立法は長期間見直されていない規定も存在し、ニーズに応じてパッチワーク的に改正されてきたともいえ、我が国における先行研究も乏しかったことから、研究開始段階において、一旦、議論の状況を整理しつつ、サイバー犯罪に対する刑法的規制のあり方を考える土壌がそろっていたといえる。

ただし、後に述べるように、IoTセキュリティの侵害に基づくサイバー・フィジカル・セキュリティの維持や保護を目的とした議論というよりは、最終的にはコンピュータ・データ化された情報を保護することに主眼を置く研究として本研究が開始されたことは、本研究を事後的にトラッキングしつつ、本研究が、サイバー・フィジカル・セキュリティの保護・維持を目的とした研究につながり得たことも示している。

### 2. 研究の目的

既に述べたように、本研究では、サイバーセキュリティ(情報セキュリティ)そのものを保護するための方策を検討することを目的とした。サイバーセキュリティとは情報の機密性・完全性・可用性(Confidentiality、Integrity、Availability)のことであり、総称してCIAといわれることもあるが維持された状態のことと定義されるが、それを刑法の観点から保護しようというときにどのような方法を用いるのがよいか。これを発見・提示することが本研究の目的であった。

### 3. 研究の方法

本研究は、そもそも情報セキュリティという分野と刑法という分野をドッキングさせた学際的な研究である。そこで、2つの分野自体において蓄積されてきている知見を独立に学ぶだけでなく、両分野を接合させる方法論を考える必要があった。

そこで代表者が着目したのが、情報とは何か?を分析することのできる情報学や記号論といった人文科学よりの議論である。情報学や記号論の知見を活かすことで、上記の2つの分野を架橋させられる知見を得て、その上で、両分野をまたいで議論をすることで、分野間の円滑なコミュニケーションを可能にするのである。

以上のように、本研究では、情報やデータ自体の概念論的調査(記号論や通信工学の知見を使用)及びサイバーセキュリティそのものに関する議論とCIA犯罪に関する諸外国の刑法的な規制の議論から得られる情報を統合する研究手法を採用した。これにより、必要な資料は法学以外の情報学・記号論といった哲学的な議論をするものにまで拡大されることになったが、膨大に存在する議論の整理が容易になる効用が期待でき、現にそうなったと考えている。諸外国の法制度を紹介する際には、一次文献を丁寧に精読し、当該国で行われている批判的な議論にも注意を払いながら、客観的で中立的になるように心がけた。

### 4. 研究成果

本研究の目的はサイバーセキュリティの保護のための刑法的検討だといえるが、サイバーセキュリティ業界の議論と刑法学のコミュニティとの間の議論には差がある状況であった。その前提には情報セキュリティの目的と刑事法学の目指すところとの間に差異があることに加え、セキュリティからみた法学の議論の複雑さ、法学から見たセキュリティの議論の技術的難解さが、双方のコミュニケーションを阻害している状況があったように思われる。そこで、研究遂行者は、一旦、議論の客体を分析するにあたり、情報やデータといった概念それ自体を記号論や分析哲学、通信工学の知見を下にして再構成し、情報とは客体の意味内容を、データとはそのような意味内容の表現と捉えることにした。そして、さらに、法学において有体物が比較的に特別視されることが多いことに着目し、存在形式の、そのような表現を媒介するものが物か電波か、といった次元を作成し、情報/データ/存在形式の3つの次元で客体を分析する「三分法」を提案した。これにより、議論の軸が明確になり、知的財産権の侵害に係る罪とサイバーセキュリティに係る罪との峻別が可能になるだけでなく、比較法的検討を行う際にも「何(情報/データ)の議論をしているのか」ということを正確に分析できるようになった。

その上で、情報セキュリティにおける情報保護のための議論を調査し、情報セキュリティの議論と刑法学の議論との際を抽出した上で、参考になる部分とそうでない部分とを分けて、例えば機密性侵害の局面においては、技術的措置が施されているのにそれを突破してサイバー攻撃を

行う場合を原則として処罰すべきではないか、という仮説を設定した。

この仮説に基づいてサイバー犯罪のうち、最も基本的な犯罪類型である無権限アクセスについて、アメリカ、イギリス、オーストラリア、ドイツ、スイス、オーストリア、及びサイバー犯罪条約の考え方を調査し、これらを紹介しつつ、無権限アクセス罪のあり方を提案した。そこでは、無権限アクセスとして、CIAの全部を保護するような法制もあったところ、C(機密性)とIA(完全性・可用性)は分けて保護するのがよく、それによる弊害も少ないこと、またCを保護する上では、パスワードや暗号化等、コンピュータ・システム内の保護措置を突破することが要件になるべきであるといった立法論的主張を展開した。

以上が本研究の主な研究成果であり(西貝吉晃「コンピュータ・データへの無権限アクセスと刑事罰(1)～(7・完)」法学協会雑誌135巻2号386頁以下、3号628頁以下、4号832頁以下、5号1213頁以下、6号1439頁以下、7号1808頁以下、8号2050頁以下(いずれも2018年))、この成果は、2018年にデジタル・フォレンジック研究会からデジタル・フォレンジック優秀若手研究者の表彰において最優秀賞を受賞し、また書籍として刊行予定である。

これに加えて、来るコネクティッドカー時代を見据え、これに対するハッキングの処罰のあり方について検討し(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」法律時報91巻4号48頁(2019年4月))、さらにSociety5.0社会を見据え、ドイツの無権限アクセス罪の議論を紹介する等した(西貝吉晃「ドイツにおける新たな無権限アクセス罪の立法論」情報法制研究(6号)36頁(2019年11月))。

ただ、そこで気づいたことは、本研究によって、「サイバー」犯罪の議論はかなり進展させることができたと思うが、「サイバー・フィジカル」・セキュリティの維持に関してはなお課題が残っていることである。例えば、CではなくIAの保護を考えていた時期に上記のコネクティッドカーシステムに対するサイバー攻撃についての考察をしたのであるが、IT化の進展が予想を上回り、IAの保護に関しては、フィジカル面を考慮しつつ、サイバー犯罪のあり方を考えるべきではないか、と思うに至ったのである(つまり、最終的に情報を保護することで一応の満足を得るサイバーセキュリティ及びサイバー犯罪の議論と、サイバー・フィジカル・セキュリティの維持の議論とを相対化する必要がある)。我が国の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の活用には限界があるかもしれない、といった問題意識に応答するための議論をサイバー空間「内」での議論で終わらせることはできない可能性があるのである。こうしたサイバー・フィジカル・セキュリティの維持に対して刑法がどう取り組むべきか、といった議論は、本研究に取り組んだことによって得た、次なる課題でもあるといえよう。

この次なる課題自体を発見できたことも成果としつつ、そして、この次なる課題に取り組んで行きつつ、引き続きサイバー犯罪本体の議論の相対化と深化を行っていきたいと考えている。

## 5. 主な発表論文等

〔雑誌論文〕 計11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 1件）

1. 著者名 西貝吉晃	4. 巻 135
2. 論文標題 コンピュータ・データへの無権限アクセスと刑事罰（4）	5. 発行年 2018年
3. 雑誌名 法学協会雑誌	6. 最初と最後の頁 273, 167
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 135
2. 論文標題 コンピュータ・データへの無権限アクセスと刑事罰（3）	5. 発行年 2018年
3. 雑誌名 法学協会雑誌	6. 最初と最後の頁 188, 79
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 135
2. 論文標題 コンピュータ・データへの無権限アクセスと刑事罰（5）	5. 発行年 2018年
3. 雑誌名 法学協会雑誌	6. 最初と最後の頁 207, 124
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 135
2. 論文標題 コンピュータ・データへの無権限アクセスと刑事罰(6)	5. 発行年 2018年
3. 雑誌名 法学協会雑誌	6. 最初と最後の頁 280, 157
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 135
2. 論文標題 コンピュータ・データへの無権限アクセスと刑事罰(7)	5. 発行年 2018年
3. 雑誌名 法学協会雑誌	6. 最初と最後の頁 230,118
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 135/2
2. 論文標題 コンピュータ・データへの無権限アクセスと刑事罰(1)	5. 発行年 2018年
3. 雑誌名 法学協会雑誌	6. 最初と最後の頁 170,73
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 135/3
2. 論文標題 コンピュータ・データへの無権限アクセスと刑事罰(2)	5. 発行年 2018年
3. 雑誌名 法学協会雑誌	6. 最初と最後の頁 226,153
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 6号
2. 論文標題 ドイツにおける新たな無権限アクセス罪の立法論	5. 発行年 2019年
3. 雑誌名 情報法制研究	6. 最初と最後の頁 36-46
掲載論文のDOI (デジタルオブジェクト識別子) <a href="https://doi.org/10.32235/al.is.6.0_36">https://doi.org/10.32235/al.is.6.0_36</a>	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 58巻2号
2. 論文標題 コンピュータ・データへの無権限アクセスと刑事罰	5. 発行年 2019年
3. 雑誌名 刑法雑誌	6. 最初と最後の頁 70 - 86
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 91巻4号
2. 論文標題 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	5. 発行年 2019年
3. 雑誌名 法律時報	6. 最初と最後の頁 48 - 53
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 85巻4号
2. 論文標題 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	5. 発行年 2020年
3. 雑誌名 日本法学	6. 最初と最後の頁 410 - 348
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 0件 / うち国際学会 0件)

1. 発表者名 西貝吉晃
2. 発表標題 コンピュータ・データへの無権限アクセスと刑事罰
3. 学会等名 日本刑法学会第96回大会
4. 発表年 2018年

〔図書〕 計1件

1. 著者名 西貝吉晃	4. 発行年 2020年
2. 出版社 有斐閣	5. 総ページ数 330
3. 書名 サイバーセキュリティと刑法 - 無権限アクセス罪を中心に -	

〔産業財産権〕

〔その他〕

日本大学法学部法律学科のページ <a href="http://kenkyu-web.cin.nihon-u.ac.jp/Profiles/135/0013465/profile.html">http://kenkyu-web.cin.nihon-u.ac.jp/Profiles/135/0013465/profile.html</a>
--

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
---------------------------	-----------------------	----