見　　解

サイバーセキュリティ研究・開発・教育における法的・倫理的課題

令和８年（２０２６年）９月 18 日

日　本　学　術　会　議

情報学委員会

サイバーセキュリティ分科会

この見解は、日本学術会議情報学委員会サイバーセキュリティ分科会の審議結果を取りまとめ公表するものである。

日本学術会議情報学委員会サイバーセキュリティ分科会

委員長	高田　広章	（第三部会員）	名古屋大学未来社会創造機構教授
副委員長	佐古　和恵	（第三部会員）	早稲田大学理工学術院教授
幹　事	岩村　誠	（連携会員）	NTT 株式会社社会情報研究所上席特別研究員
幹　事	松浦　幹太	（連携会員）	東京大学生産技術研究所教授
	相原　玲二	（連携会員）	広島大学上席特任学術研究員／安田女子大学理工学部教授
	阿部　正幸	（連携会員）	NTT 株式会社社会情報研究所フェロー
	稲見　昌彦	（連携会員）	東京大学先端科学技術研究センター教授
	井上美智子	（連携会員）	奈良先端科学技術大学院大学先端科学技術研究科情報科学領域教授
	位野木万里	（連携会員）	工学院大学情報学部コンピュータ科学科教授
	大倉　典子	（連携会員）	環太平洋大学国際経済経営学部特任教授／芝浦工業大学名誉教授
	岡部　寿男	（連携会員）	京都大学学術情報メディアセンター教授
	柴山　悦哉	（連携会員）	大学共同利用機関法人情報・システム研究機構理事
	須藤　修	（連携会員）	東京大学名誉教授／中央大学 ELSI センターアドバイザー／OECD Expert Group of AI Futures メンバー
	砂原　秀樹	（連携会員）	麗澤大学工学部教授
	住井英二郎	（連携会員）	東北大学大学院情報科学研究科教授
	竹房あつ子	（連携会員）	大学共同利用機関法人情報・システム研究機構国立情報学研究所教授
	谷　誠一郎	（連携会員）	早稲田大学教育・総合科学学術院教授
	中川　晋一	（連携会員）	一般社団法人情報通信医学研究所代表理事／所長
	原田　悦子	（連携会員）	筑波大学名誉教授／客員教授／株式会社イデアラボリサーチディレクター
	盛合　志帆	（連携会員）	国立研究開発法人情報通信研究機構執行役／サイバーセキュリティ研究所所長
	後藤　厚宏	（連携会員（特任））	情報セキュリティ大学院大学教授
	宮地　充子	（連携会員（特任））	大阪大学大学院工学研究科栄誉教授

本見解の作成にあたり、以下の職員が事務及び調査を担当した。

事務	新田　浩史	参事官（審議第二担当）
	渡邊英一郎	参事官（審議第二担当）（令和８年７月から）
	角田美知子	参事官（審議第二担当）付参事官補佐
	櫻井　　碧	参事官（審議第二担当）付審議専門職
調査	辻　　政俊	上席学術調査員

要　　旨

１　作成の背景

現代社会において情報システムは人命や社会インフラを支える重要基盤となっているが、サイバー攻撃の脅威は深刻化しており、防御側が攻撃者の思考を先回りする「踏み込んだ研究」（脆弱性の能動的な探索・分析、マルウェアの挙動解析、実環境に近い条件での攻撃シナリオの再現・評価等）が不可欠となっている。しかしながら、こうした研究活動は、不正アクセス禁止法や刑法（ウイルス作成・提供罪等）などの法的リスクへの懸念、あるいは研究成果の公開に伴う倫理的配慮の難しさから、萎縮してしまうケースがある。本見解は、これらの法的・倫理的課題を整理し、サイバーセキュリティ分野の研究・開発及び教育を活性化し、安全な社会基盤の構築に寄与するための提案を行うものである。

２　現状及び問題点

法的側面では、正当な研究目的であっても、管理者の承諾を得ない調査やマルウェアの取り扱いが、現行法（不正アクセス禁止法、ウイルス作成・提供罪等）に抵触する懸念があり、正当性要件の解釈も必ずしも一定・共有されていない。また、リバースエンジニアリングが契約により禁止され、脆弱性調査が阻害される問題もある。

倫理的側面では、医学研究を範とする従来の倫理規範がサイバーセキュリティ特有の課題（攻撃手法の評価やネットワークへの影響等）に適合しない場合がある。脆弱性に関する情報の取り扱いについては、責任ある開示の枠組みがあるものの、調整の長期化により研究成果の公表が遅れ、研究者の評価が損なわれるなどの課題が指摘されている。教育的側面では、技術の悪用を防ぐ倫理指導が不可欠であるが、具体的なカリキュラムや体制の構築は容易ではなく、高度な人材育成の妨げとなるおそれがある。

３　提案の内容

(1) 相談機関の設置

サイバーセキュリティ分野の研究・開発・教育における個別の法的・倫理的課題について、研究者等が相談を持ちかけ、適切なアプローチを共に議論する相談機関（助言委員会）を、公的資金により設置すべきである。当該機関は、サイバーセキュリティ研究者・開発者・教育者に加え、法律家や関係省庁を含む多様なステークホルダーで構成し、研究計画の法的・倫理的妥当性の検討や、責任ある開示の実践やサイバー攻撃手法の教育における留意点などに関する助言を行うことで、研究者・開発者・教育者の萎縮を防ぎ、適切な研究・開発・教育活動を支援する。

(2) 判断基準を作る場の整備

個別事例への対応にとどまらず、サイバーセキュリティ分野の研究・開発・教育における法的・倫理的問題に関する普遍的な「判断基準」を策定・維持するための協議・検討の枠組みを整備すべきである。ここでは、相談機関で蓄積された事例をもとに、研究者・開発者・教育者、消費者、規制官庁などが集い、社会的合意形成を図りながら基準を作成する。これにより、法解釈の明確化や必要なルール形成を促し、予見可能性の高い研究環境を実現する。

(3) 基準の整備・普及

マルウェアの管理基準や、サイバーセキュリティ教育における倫理カリキュラムなど、一部の専門家の間では事実上の標準となっている事項については早急に明文化し、普及させるべきである。これらの知見を広く共有することで、新規参入者の障壁を下げると共に、意図せぬ法令違反やインシデントを防ぎ、健全な研究・開発・教育活動を促進する。

目　　次

１　背景

現代社会は、医療、金融、交通、エネルギー、行政サービスに至るまで、その基盤を情報通信システムに強く依存している。社会全体のデジタル化とIoT機器の爆発的な普及は利便性を高める一方、サイバー攻撃の脅威をいっそう深刻化させている。

初期のサイバー攻撃では、企業秘密の窃取や示威行為を目的としたウェブサイト改ざんが多くみられた。しかし今日では、その被害は人命や社会インフラにも及んでいる。例えば、病院のシステムがランサムウェア攻撃を受けて停止し、救急患者の受入れ停止や搬送先変更が生じ、患者の死亡との関連が疑われたケースがある[1]。また送電線網へのサイバー攻撃により、大規模停電が発生するといった社会の混乱を招く事例も報告されている[2]。

こうした被害が発生する要因として、サイバーセキュリティにおける防御コストの増加がある。攻撃側は一か所でも攻撃の糸口を見つけられれば良い一方、防御側はすべての隙をふさぎ続ける必要があるが、昨今の情報システムは大規模化・複雑化が進むことで、相対的に防御側のコストが増大している。そこで求められるのは、攻撃者視点に立ち、攻撃の糸口を減らすと共に、侵入を許した際は、迅速な復旧により被害を最小化するという考え方である。そのためには、未知の脆弱性を能動的に探索・分析する研究、マルウェア挙動を詳細に解析して攻撃者の意図や手口を解明する研究、実環境に近い条件で攻撃シナリオを再現・評価する研究など、防御側が攻撃者の思考を先回りする「踏み込んだ研究」が不可欠である。サイバーセキュリティでは、この攻撃的視点から得られる知見こそが、現実の脅威を先取りした堅牢な防御技術と効果的なインシデント対応を生み出す源泉となる。

一方で、こうした重要な「踏み込んだ研究」は、法的・倫理的な論点により萎縮してしまっているケースがある。

法的側面では、攻撃ツールやマルウェアの取り扱いにおいて、正当な利用目的が求められる。その正当性を担保する客観的な根拠として、安全管理体制や運用ルールの整備が必要となるが、組織内の整備が遅れていたり、関連法令の理解が不十分であったりすることが、計画段階からの萎縮につながり得る。

倫理面では、学術的な成果公開の迅速性と、社会的影響に配慮した「責任ある開示（Responsible DisclosureまたはCoordinated Disclosure)」との調整が難しい。脆弱性の発見・報告が対象製品・サービスの開発者に必ずしも歓迎されず、開発者からの反論を招く懸念が、サイバーセキュリティ研究への新規参入の障壁となる場合もある。教育面でも、技術の悪用を防ぐ倫理指導は不可欠だが、教育対象の年齢・経験や技術の悪用可能性に応じた内容設計が必要となるため、その具体的なカリキュラムや体制の構築は容易ではなく、結果として高度なセキュリティ人材の育成や社会実装の遅れにつながりかねない。

本見解は、これらの法的・倫理的課題に関する事例と現状の取り組みを整理

し、サイバーセキュリティ分野の研究・開発及び教育を活性化するための提案を行うものである。

2　課題意識・事例・現状の取り組み

(1)　法的問題

サイバーセキュリティ分野の研究・教育は、その定義から、情報システムに対する攻撃や不正侵入への対応及びそれらの防止を主な目的としている。そのため、必然的に、攻撃や不正侵入そのものを研究し、しばしば既存の攻撃・不正侵入手法を再現あるいは新たな手法を開発、あるいは情報システムのセキュリティ上の欠陥（脆弱性）を発見することとなる。

一方、攻撃・不正侵入行為を行った者は、各国の法令に基づき刑事責任を問われ、あるいは民事上の損害賠償責任を負うことがある。わが国では特に不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）、刑法第 168 条の２及び第 168 条の３（不正指令電磁的記録に関する罪、いわゆるウイルス作成・提供罪）、刑法第 233 条（偽計業務妨害罪）、著作権法等がサイバーセキュリティ研究・教育に関係する。

例えば実在の情報システムにおいて脆弱性の存在が疑われ、その存在を確認したいが、その情報システムの管理者の承諾が得られない場合、承諾を得ずに脆弱性を実際に確認すると、不正アクセス禁止法第３条（不正アクセス行為の禁止）に抵触して三年以下の拘禁刑又は百万円以下の罰金に処されるおそれがある（同法第 11 条）。なお、同条には「業務その他正当な理由による場合を除いては」といった例外も規定されておらず、管理者の承諾を得ない不正アクセスを刑法第 35 条の正当業務行為として合法とした事例も見当たらない。（国立研究開発法人情報通信研究機構法に基づき、同機構が行う特定の調査について認められた例外は、一般のサイバーセキュリティ研究には適用されない。）

ウイルス作成・提供罪には「正当な理由がないのに」「人の電子計算機における実行の用に供する目的で」といった規定があるが、その「正当な理由」や、使用者の「意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令」といった規定の解釈が（警察庁[3]及び法務省[4]の解説や、後述の比較的最近の最高裁判所判決はあるものの）関係者・当事者間で必ずしも一定・共有されていない[5]。そのため、例えば技術的には素朴で対処も比較的容易な、いわゆる無限ループのプログラムへのリンクを投稿した未成年者らがウイルス提供罪の疑いをかけられ補導等されたり[6,7]、計算機への技術的影響としては通常のインターネット広告等と大差のない、いわゆる暗号通貨採掘プログラムの一種を、自身の Web ページの閲覧者にスクリプトとして実行させた個人らが検挙され、最高裁判所まで至って裁判官全員一致の意見により不正性が否定され無罪と判決されたり[8]といった事例が発生している。IT セキュリティ企業の社員がウイルス保管の容疑で逮捕されたり[9]、ごく初歩的なプログラムを掲載した Web サイトの管理者が罰金刑を受けたり[10]といった例もある。さらに過去には、技術的には特段の問題のないプログ

ラムを個人が作成・実行したところ、そのプログラムによりアクセスされた公共の情報システム側の問題により障害が発生し、プログラムを作成・実行した側の個人が偽計業務妨害の容疑で逮捕され、20 日間にわたり勾留される[11]といった事例も発生している。サイバーセキュリティを担当する自衛官が訓練のために作成した模擬的なプログラムがマルウェアとして検出・立件され、最終的には不起訴処分となったが退職に至ったケースもある[12]。

一方、研究の一環として他者のプログラムを解析する（いわゆるリバースエンジニアリングを行う）場合、著作権法上の複製権等を侵害するおそれがあったが、日本では 2018（平成 30）年の改正により一定の例外が認められることとなった（無論、著作権者あるいはその他の者の利益を不当に害する場合は、著作権法あるいは他の法令に違反するおそれがある）[13]。日本の不正競争防止法においても「技術的制限手段の試験又は研究」に関しては例外が規定されている（同法第 19 条第 1 項第 10 号）。しかしながら、ソフトウェアの利用許諾契約等により、その利用者に対して当該ソフトウェアのリバースエンジニアリングが禁止されるケースは依然として多く、脆弱性の発見・報告・対処等の妨げとなりうる。

国外においては、例えば電子書籍の著作権保護の脆弱性を米国のカンファレンスで発表したプログラマが、Digital Millennium Copyright Act (DMCA)を理由として連邦捜査局(FBI)に逮捕されたり[14]、Linux で DVD を再生するためのソフトウェアを公開したノルウェーの当時 15 歳の個人が家宅捜索を受け起訴されたり[15]といった事例も多い。また、セキュリティ脆弱性の研究発表が司法により差し止められた複数の事例[16,17]もある。

これらの問題は、技術者・研究者らに対して、正当な研究・教育目的で行った行為であっても法律違反と評価されたり、不当に捜査・逮捕等の対象となったりするのではないかという不信や不安を与え、サイバーセキュリティ研究においても懸念が生じている。いわゆる正当性要件の明確化等により、そのような懸念を解消し、健全かつ円滑なサイバーセキュリティ研究に資する制度の整備が望まれる。

(2) 倫理的問題

情報処理研究における倫理的問題は、医学における倫理規範をもとに考えられてきた。すなわち、人間を対象とする医学研究の倫理規範であるヘルシンキ宣言[18]から、具体的行動基準としてベルモントレポート[19]で人を対象とする研究における倫理骨子が確立された。情報処理の分野でも各学会の倫理規範が策定され、より具体化した行動規範としてメンローレポート[20]で、人格の尊重、恩恵、正義、法と公益の尊重の 4 点を遵守するとされた。本基準は情報処理全般の倫理基準として用いられ、各種学会においても同基準に基づいたチェックシートにより審査が行われてきた。しかし研究内容の複雑化・

多様化が進行し、ヒトを対象とする研究を想定してきた同基準を一律に適用することが難しい事例が増加しており、それぞれの学術団体（学会、査読委員会ならびに組織倫理委員会：IRB）が個別に判断せざるを得ないことから、判断の一貫性や予見可能性が課題とされている[21]。

①　サイバーセキュリティ研究における倫理規定の問題点

わが国においてもメンローレポートの規定に準拠すべく学会を中心として解決案が模索され、研究における倫理問題のチェックリストが公開され、相談窓口の運営も行われているが倫理原則を実運用の研究に適用する際の課題も指摘されている[22]。例えばネットワーク上の大量のパケットを収集し内容を解析するようなサイバーセキュリティ研究では、モニタリング対象者全員にインフォームドコンセント（説明と同意）を得ることができないなど問題も生じている。このような事例に対し従来用いられてきた倫理問題に関するチェックシートの他にノレッジベースを用いて判定を試みるなど新規手法も提案されている[23]。

また、メンローレポートの規定に従う場合、例えばシステムの脆弱性に関して研究した結果を「法と公益の尊重」に従って責任ある開示の手順で公開した場合であっても、システムを使用するユーザの「恩恵」を侵害する可能性が指摘されている。例えば脆弱性を発見したシステムが患者の生死を左右する医療システムである場合、システムの脆弱性を公表しそのシステムを一時的にせよ停止するなどの措置が必要になれば患者生命は危険に晒される。研究成果としての脆弱性に関する情報をどう扱うのかについて更なる検討が必要であることが指摘されている[24]。

さらに、オープンソースソフトウェア（OSS）コミュニティにおけるコードレビュープロセスを評価するために、Linuxカーネルに脆弱性入りパッチを混入させることによって調査した論文が国際会議に採択された後、Linuxカーネルコミュニティ、同国際会議プログラム委員会、著者らの所属大学において議論された結果として取り下げとなった事例がある[25]。本例は研究者が公知せず脆弱性入りパッチを混入させ、これが取り除かれていく期間までを調査することにより、OSSのコードレビューの脆弱性を指摘、パッチの提供者の身元確認、説明責任などの問題点を指摘するなど、研究成果としては価値があるとされたが、結果的に研究方法の倫理上の問題から取り下げとなった[26]。現在、主に医学や心理学などヒトを対象とする一般的な研究を前提として設置されている組織倫理委員会（IRB）において、情報処理・通信工学分野の中でも高度な知識と専門性が求められるサイバーセキュリティ分野特有の手法や影響を適切に評価できるよう、その専門性を高める必要が指摘されている[27]。

②　倫理問題の多様化と複雑化、教育のあり方について

近年、サイバーセキュリティ事案の多様化や、関与者の低年齢化などが社会問題化してきており、本分野の技術者・研究者の倫理教育の必要性と倫理意識向上の必要性も高まってきている。

2023年には、わが国でセキュリティ技術者の養成を目的として実施されているSecHack365の修了者が、不正に入手したクレジットカード番号の不正使用に関与したとされる事案が発生した。同講座では法と倫理に関する教育を継続的に実施しているが、今後も教育内容の更なる検討が必要であるとコメントしている[28]。また、2025年に発生した中高生による不正アクセス事案[29]は、生成AIの悪用により技術的ハードルが低下したことを背景としており、高等教育機関の専門教育以前の段階、すなわち初等中等教育からの倫理教育が必須であることを示唆している。

一方で、事案を起こした人材の更生や、善意の研究活動の保護という観点も重要である。1988年のモリスワーム事件[30]では、有罪判決を受けた学生が後に研究者として大成し、サイバーセキュリティ分野に貢献した例がある。わが国においては、こうした人材に対する特別な再教育・育成の仕組みは未整備であるが、事案の重大さと反省を踏まえた上での人材活用の道筋も模索されるべきである。

③　本分野における倫理問題の複雑化への対応の必要性

研究成果の公開は研究者にとって業績評価の基盤であるが、サイバーセキュリティ分野においては、その公開自体が新たな攻撃手法の流布というリスクを孕んでいる。結果として詳細な手法を非公開とせざるを得ないケースもあり、第三者による検証（再現性の確認）や正当な業績評価が妨げられ、学術分野としての発展の障害となることも懸念される。

本分野における倫理的課題への対応として、従来のメンローレポートに基づく枠組みに加え、(１)各研究における倫理的配慮、(２)研究が倫理的に許容される範囲で行われたかの監視・管理・公開、(３)セキュリティ事案発生時の対応、などの点が求められる。これらを実現するための参考となるのが、医学分野における臨床研究の枠組みである[31]。具体的には、研究開始前の手続き、方法の公開と審査、参加者への説明と同意、責任委員会による研究の開始・中断・継続・終了の管理など、安全な研究体制を整備することが必要である。ただし、医学においても、1947年のニュルンベルク綱領、1964年のヘルシンキ宣言に始まる研究倫理の議論は、その後も1979年のベルモント・レポートを経て、2000年代に入ってもヘルシンキ宣言の改訂が繰り返されるなど、長期にわたって継続しており、倫理規範の確立は一朝一夕に進むものではない。現在の研究者の研究モチベーションや生産性を低下させるのではなく、それらを保護しつつルールを浸透させるなど、深遠な配慮が求め

られる。

(3) 現状の取り組みと課題

サイバーセキュリティ研究には、研究計画段階での倫理的適切性の確保に加え、研究成果の公開によって生じうる社会的影響への配慮という二つの倫理的観点が求められる。本節では、まず研究実施前の倫理審査の現状と課題を整理した上で、脆弱性研究に特有の情報公開プロセスである責任ある開示（Responsible DisclosureまたはCoordinated Disclosure）の必要性と課題について述べる。

① 研究計画段階における倫理審査・相談体制

多くの大学では研究倫理審査委員会が設置され、研究計画が倫理的に適切かどうかを事前に判断する仕組みが整備されている。また、海外の主要なセキュリティ会議では、論文投稿時に「研究倫理審査委員会による承認の有無」に加え、研究の実施過程及び研究成果公開の際にどのような倫理的配慮を行ったかの記述が義務付けられている。これにはデータ管理や参加者保護だけでなく、発見した脆弱性の公開方法・公開時期に関する配慮も含まれる。すなわち、研究計画段階と研究成果公開段階の双方において倫理的責任が問われる。

しかし日本国内の研究倫理審査委員会は、医学系研究の生命倫理を主たる対象として発展してきた歴史的経緯があるため、その専門性から、攻撃手法の評価、ネットワークへの影響、脆弱性の意図的利用といったサイバーセキュリティ固有の論点には十分に対応できない場合がある。また、自組織への批判を避けるために研究を制限する方向に判断が傾くことも懸念される。さらに、大学や研究機関がサイバーセキュリティに特化した倫理審査能力を独自に整備することは、リソース面からも容易ではない。

このような状況を補完する取り組みとして、国内学会による自主的な試みが進んでいる。

前述したように、情報処理学会コンピュータセキュリティシンポジウム（CSS）では、投稿者が事前に確認できる「サイバーセキュリティ倫理に関するチェックリスト」を作成し、必要に応じて倫理的妥当性について相談できる窓口を設けている[1]。このチェックリストは（１）倫理綱領の遵守、（２）機微情報の適切な扱い、（３）研究成果公開によるネガティブな影響の検討と対処、の三つの観点から構成されており、特に（３）は国際的に議論される責任ある開示と密接に関係している。これに関連する取り組みは、「サ

[1] 情報処理学会コンピュータセキュリティ研究会（CSEC）や電子情報通信学会 暗号と情報セキュリティシンポジウムも本チェックリストを用いて投稿前の確認を推奨している他、セキュリティ関係の論文誌での活用も広がっており、英語化もされている。

イバーセキュリティ研究における倫理的な研究プロセスについて」というサイトにまとめられている[32]。

さらに、電子情報通信学会（IEICE）では、倫理委員会が主体となって「倫理事例集」を作成し、研究者が倫理的判断を当事者意識をもって考えられるよう支援している。この事例集は、過去に実際に発生した問題や今後起こり得る具体的なケースを題材としており、単一の「正解」を提示するのではなく、さまざまな観点から議論できるよう構成されている。これにより、研究者が直面しがちなグレーゾーンや現場判断の難しさを踏まえた倫理的検討が促進されている。

なお、これらの国内学会による取り組みは、研究計画段階だけでなく、研究成果の公開段階における倫理的責任にも対応しており、次節で述べる責任ある開示/協調的開示の概念とも整合しているベストプラクティスであると言える。

②　責任ある開示

サイバーセキュリティ研究では、研究の結果として既存製品やサービスに脆弱性が存在することが明らかになることがある。この情報が修正前に公開されると、製品利用者が攻撃を受ける危険性がある。そこで、海外では「責任ある開示（Responsible Disclosure）」という枠組みが提唱されてきた[33]。

責任ある情報開示とは、研究者が脆弱性を公表する前に、影響を受ける可能性のある企業に事前通知し、修正の時間と機会を提供するものである。しかし企業側の対応が遅れ、研究成果が公開できないまま長期にわたり停滞する事例が相次いだ。これは、製品利用者が脆弱性のある製品を使い続けることとなる。これは「研究者のみが責任を負う」構造の限界を示している。

この問題を踏まえ、最近では、「責任ある」という言葉が「発見者側だけに責任を押し付けている」というニュアンスを含んでしまうため、より協力的な姿勢を強調した「協調的開示（Coordinated Disclosure）」という呼び方が主流となった。ISO/IEC 29147（脆弱性開示）とISO/IEC 30111（脆弱性ハンドリング）は、この協調的開示を実現するためのプロセスの規格である。

日本では、経済産業省の告示に基づき、IPAとJPCERT/CCが「情報セキュリティ早期警戒パートナーシップガイドライン」を策定・運用しており、発見者・製品開発者・調整機関の三者間における脆弱性情報の適切な流通と調整を担っている。しかし、窓口が一本化されることで報告がここに集中する結果、調整プロセスが長引いているという課題が指摘されている。これにより研究成果の公開が遅れることで、学術業績にならない期間が生じるという懸念点がある[2]。国際的に競争が激しい分野において、日本の研究者が不利と

[2] 報告に先立って、研究成果の公表に支障がないか、IPA や JPCERT/CC に相談することは考えられる。

ならないようにすることが必要である。一方、深刻な脆弱性に対して、企業の対応が遅れるようであれば、製品利用者を脆弱な環境に晒し続けることを意味する。社会に公開することによって、企業の速やかな対応を後押しできる可能性がある。IPAやJPCERT/CC等の調整機関への追加的予算措置を含め、脆弱性情報の受付、関係者間の調整、公表に至るプロセスを迅速に進める必要がある。

以上のような取り組みがある一方で、責任ある開示に関する理解・実践が不足している研究者も少なくない。そのため、研究者への普及啓発を含め、その理解と実践をより一層促進するための施策が必要である。

さらに、これら制度面の改善と同時に、研究者の評価のあり方も見直すべきである。責任ある開示のプロセスは、社会全体のセキュリティ向上に直結する重要な活動である。従って、脆弱性を発見したという技術的な成果にとどまらず、調整プロセスを通じて脆弱性の修正に寄与した貢献そのものを、高い学術的業績として正当に評価する文化の醸成も求められる[3]。

(4) 具体的な検討課題

この節では、現行法令や制度に対して検討が求められる具体的な課題の例について、研究・開発に関するものを中心に述べる。教育に関する具体的課題については、倫理指導やカリキュラム整備の観点から他の節で扱っている。

① リバースエンジニアリングを不当に制限しない制度の整備

ソフトウェアの脆弱性調査においてリバースエンジニアリングは不可欠な手法であるが、前述のように、個別のライセンス契約等によって禁止されることが少なくない。これは脆弱性の発見・報告・対処を阻害する要因となっている。従って、ライセンス契約等におけるリバースエンジニアリング禁止条項を無効とする、あるいはそのような条項を設けること自体を禁止するなど、正当な脆弱性調査を妨げないための法的な制度整備を検討することが考えられる。

なお、米国のデジタルミレニアム著作権法でも、相互運用性の確保を目的とするリバースエンジニアリングや、暗号研究・セキュリティテスト等について一定の例外が設けられているが、契約でこれらの法定例外の適用を排除できないと明確にされているわけではない[34]。一方、EUのコンピュータプログラム指令では、ソフトウェアの相互運用性を確保するためのリバースエンジニアリング（デコンパイル）が認められており、これに反する契約条項は無効とすることが明文で規定されている。

[3] 例えば、JPCERT/CC では、脆弱性の報告などに関して研究者やエンジニアの貢献に対して感謝状を贈っている（https://www.jpcert.or.jp/award/appreciation-award.html）。

②　開発者に対する脆弱性の対応・公表義務の是非

現状では、研究者が脆弱性を発見し開発者に報告した場合であっても、開発者がその脆弱性に対応し、またはそれに関する情報を公表する法的義務は一般には課されていない。そのため、悪影響が懸念される脆弱性を研究者が報告しても、開発者が正当な理由なく対応も公表も行わず、脆弱性が放置されるケースがあり得る。この場合、研究者は、利用者への被害拡大を避けるために直ちに詳細を公表することも困難であり、結果として研究成果の公表や社会への注意喚起が停滞することになる。

しかしながら、社会的に影響の大きい脆弱性については、それを放置することが重大な社会的損失を招くおそれがあることから、開発者に対して開示方法に留意しつつ対応・公表することを法的に義務付けることも考えられる。一方で、そのような義務は、開発者の負担を過度に増やすという懸念もある。なお、開発者に対する義務のあり方を検討する際には、製品・サービスを組み込んで運用する者との関係にも配慮する必要がある。

開発者の対応・公表に関する義務が明確化されれば、研究者が発見し報告した脆弱性について、開発者による修正、利用者への周知、及び研究成果の公表に至る道筋がより明確になる。また、開発者が合理的な期間内に対応・公表を行わない場合には、研究者による独自の情報公開の正当性を判断する上での基準も明確になり、健全な緊張関係の下でセキュリティ研究が促進されることが期待できる。

なお、EUのサイバーレジリエンス法では、悪用されている脆弱性について、極めて短い期間で公的機関に報告することが義務付けられている一方、これが開発者にとって過度な負担になるのではないかという声もある。

③　研究成果が公開できない場合の評価・救済スキームの構築

研究者が社会的に重大な影響を与える脆弱性を発見した場合、その成果を直ちに公表できず、公表が制限される可能性がある。一方で、研究者にとって成果の公開は極めて重要であり、公開できないことは研究者としての評価やキャリアに大きな影響を及ぼす。特に大学院生や学位取得を目指す研究者の場合、研究成果を発表できないことは学位取得に直接の支障が生じるため、このようなリスクを避けるべく研究テーマの選択が制約されるおそれがある。

この課題を解決するためには、責任ある開示に関する基準を整備することや、前述した脆弱性修正に寄与した貢献を学術的業績として評価することに加えて、それでもなお成果が公開できない場合において、研究者が正当に評価され、活動が適切に補償または救済される仕組みを構築することが望まれる。

３　提案

この章では、サイバーセキュリティ分野の研究・開発及び教育の活性化のために、取り組むべきことについて提案する。まず(1)では、個別の案件について相談を受け、助言を行う機関の設置を、(2)では、個別の相談・助言事例を元に、法的・倫理的問題に関する判断基準を作る場の整備を提案する。(3)では、すでに事実上の基準があるものについては、早急に基準の整備・普及を進めることを提案する。これらの提案を進めるにあたっては、研究の自由と社会的責任の両立を図り、関係する多様なステークホルダーへの影響に十分配慮することが重要である。

(1)　相談機関の設置

サイバーセキュリティ分野の研究・開発及び教育における個別の法的・倫理的課題について、研究者・開発者・教育者が相談を持ちかけ、研究・開発・教育を推進するにあたっての適切なアプローチを共に議論する相談機関（助言委員会）を、公的資金により設置することを提案する。その具体的な設置・運営主体や関係機関の役割分担については、関係省庁・規制当局、学術機関、学会等が連携して検討することが望ましい。

生命倫理分野ではすでに、学術機関ごとに研究者向けの相談・審査機関が設けられており、現行法令や倫理的観点に基づき個別の事例が議論され、実効的に機能している。これらの審査は、主として研究計画時点における倫理的妥当性の確認を目的としている。一方、サイバーセキュリティ分野においては、研究計画時点での判断に加え、研究の過程で得られた成果をどのように取り扱い、公開するかといった点も重要な論点となる。しかしながら、サイバーセキュリティ分野においては、研究グループの規模や分布を踏まえると、学術機関ごとに同様の機関を設置するのは非現実的であり、多様な事例を通じた経験の蓄積も難しい。そこで、大学・研究機関や企業等の関係者が共同利用できる機関であることが望ましい。

学会では、研究者による自発的な活動として、例えば情報処理学会のコンピュータセキュリティシンポジウムで見られるように、学会発表に関連する研究倫理上の課題について相談できる窓口が設けられ、活動実績を積み重ねながらベストプラクティスを築いている（２章(3)節参照）。海外動向に精通した研究者からの助言が提供されることで、若手研究者が自らの研究内容を内省する契機ともなっている。しかしながら、研究者が限られたリソースの中でボランティアベースで設置・運用していることから、継続性や対応可能な範囲に限界がある。従って、この相談機関を、このような学会活動の実績も踏まえつつ、公的資金により運営される常設の機関として整備することが望ましい。

この機関には、サイバーセキュリティ研究者・開発者・教育者に加え、現行法に精通した弁護士、関係省庁・規制当局の実務者など、関連する多様なステ

ークホルダーが参画し、以下の役割を担うことが望ましい。

1） 研究者・開発者・教育者からの相談に対し、法令を遵守しつつ、わが国として最大限の成果が得られるよう実施方法に対して助言を行うこと。

2） 対象となる実施計画に対し、法的・倫理的な観点から問題の有無を検討・議論すること。

3） 責任ある開示を含むサイバーセキュリティ固有の課題について相談者自身が理解を深め、適切な実践につなげるための学びと内省の機会を提供すること。

なお、この機関による助言は法的拘束力を有するものではなく、助言を受けたことにより、相談者その他の関係者が刑事上又は民事上の責任を当然に免れるものではない。

このような相談・議論の対象となる研究は構想段階であることが多いため、関係者には一定期間の秘密保持義務を課すことが必要である。

また、この相談機関は、サイバーセキュリティに関するあらゆる研究・教育活動に関する相談を一律に受け付けることを想定するものではない。大学・研究機関や学会における一次的な相談・判断を前提とし、それらでは対応が困難な法的・倫理的判断を要する事案や、研究成果の公開方法を含む高度かつ横断的な検討が必要な事案を主な対象とすることが想定される。併せて、サイバーセキュリティ関係者一人ひとりが自ら内省し、倫理的に研究・教育に取り組める基礎的な判断力を育成する取り組みを支援することも重要である。このような段階的な相談体制と研究者の基礎的判断力の育成を併せて進めることで、限られたリソースの中でも実効的に機能する体制を確保し、相談が過度に集中することによる機能不全を防ぐことが重要である。

研究・開発分野における検討の例として、現行のサービスの脆弱性を明らかにするための調査手法（例えばネットワークスキャンやクローリング）の妥当性、攻撃シナリオの再現など疑似攻撃を伴う研究、SNSアカウントの大量作成や外部サービスの利用規約に抵触する可能性のある利用を伴う調査などが挙げられる。

また、教育分野における助言の一例として、サイバー攻撃に関する演習を行う際に、演習環境をどのように整備すれば良いかや、受講者に事前に教えておくべき前提知識は何か、あるいは不幸にして受講者が受講後に知識を不正利用した際にどのような対応をすべきか、などが考えられる。

なお、この相談機関は、大学や研究機関における既存の相談・審査機関を代替するものではない。大学・研究機関は、研究者・教育者に最も近い立場として、研究構想の初期段階における一次的な相談対応や、学内ルールとの整合性確認、研究・教育の実施に関する最終的な責任を担う主体である。一方で、法的解釈や社会的影響の評価が困難な事案、あるいは研究成果の公開方法を含む高度な判断が必要な事案については、大学・研究機関や企業等の関係者が共

同で利用できる相談機関に接続することで、より適切な判断が可能となる。このような二層的な役割分担により、研究者の負担を過度に増やすことなく、研究の自由と社会的責任の両立が図られる。

(2) 判断基準を作る場の整備

サイバーセキュリティの研究・開発及び教育における法的・倫理的問題に関する判断基準は、すでに事実上あるもの以外は、関連する異なるステークホルダーが集い、社会的合意形成を伴って作られ維持・更新されるべきである。そこで、(1)で提案した個別事例を扱う相談機関とは別に、相談機関で蓄積された事例や国内外の動向を踏まえ、法的・倫理的判断基準を継続的に検討・更新するための協議・検討の枠組み（以下「判断基準を作る場」という。）を整備することを提案する。

判断基準を作る場では、相談機関が扱った個別事例をベースに一般化するなどの検討を行う。そして、法解釈の明確化や、場合によっては新しい法律（ルール）作成を促す提案をするなどして、変化の激しいサイバーセキュリティ分野において相談機関における個別事例の検討に参照できる判断基準を提供する。倫理的問題に関しては、国際的動向を踏まえた対応が求められる。

この判断基準を作る場に集うべきステークホルダーには、消費者、組織的に取り組む企業だけでなく個人で活動するエンジニアも含むソフトウェア開発者、研究者、教育者、規制官庁が含まれる。判断基準を作る場の整備後ではなく整備過程から、これらのステークホルダーが関与することが望ましい。

判断基準を作る場が有効に機能すれば、学会における自発的な活動や、相談/審査機関の生産性も高まることが期待される。また、研究成果を社会に発信し還元する過程だけでなく、研究を計画する段階から法的・倫理的問題に適切かつ効率的に対応することが容易になると期待される。

教育では、判断基準を作る場が有効に機能すれば、安心して効果的な演習を実施することが容易になるなど、実践的な教育の水準向上が見込まれる。具体的な教育プロジェクトに参画した大学等がサイバーセキュリティを学ぶ場を共有する取り組みは、例えば「成長分野を支える情報技術人材の育成拠点の形成(enPiT)」のセキュリティ分野で見られるように、実践的な教育の水準向上に貢献してきた。判断基準を作る場が有効に機能し、サイバーセキュリティ教育の普及がさらに進めば、将来のサイバーセキュリティ確保を支える礎となるであろう。

(3) 基準の整備・普及

整備すべき基準の中には、すでに事実上の基準があるにもかかわらず、それが明文化され普及するに至っていないものもある。そのような基準については、(2)で提案した判断基準を作る場の整備を待たずに、基準の整備・普及を

早急に進めることを提案する。

サイバーセキュリティの研究・開発及び教育を遂行するにあたっては、関連法規やガイドラインの遵守に加え、ステークホルダーに悪影響を及ぼさないために追加の配慮が求められる。しかしながら、こうした配慮に必要な知見は、分野に精通した研究者にとっては当然のことであっても、必ずしも広く共有されているとは限らない。このような状況は、他分野からの新規参入を妨げる一因となるだけでなく、適切な対応を怠ることで思わぬインシデントを引き起こす危険性もはらんでいる。

例えば、マルウェア（コンピュータウイルス）を取り扱う研究がある。マルウェアの扱いに際してまず留意すべきこととして、「不正指令電磁的記録に関する罪」がある[4]。これは、正当な理由なくマルウェアを作成・提供したり、他者の意図に反して実行させる目的でそのソースコードを取得・保管したりする行為を処罰の対象とするものである。こうしたマルウェアの取り扱いは、正当な研究・開発・教育目的であり、正当な理由が認められる場合には、同罪の構成要件を満たさない。しかしながら、現状では、マルウェアを扱う際の正当性要件が具体的な手続きとして十分に定義されておらず、マルウェアの取得・保管等をためらわせる原因になっている。分野に精通した研究者は、マルウェアの管理基準を整備し、それを遵守することで、正当性を客観的に示すための配慮を行っているが、そのような管理基準は広く共有されているわけではない。そこで、広く認められた管理基準を明文化し、普及させることが必要である。

また、マルウェアを研究・開発・教育目的で取り扱う際には、法令の遵守に加え、周囲に危害を与えないための技術的な基準も必要となる。例えば、マルウェア分析には、コード等を調査する静的解析、隔離されたサンドボックス環境で実行時の振る舞いを観察する動的解析、既知の特徴量に基づくシグネチャ解析など、多種多様なアプローチが存在する。分析実施の際は、研究・開発・教育の各目的に従い、技術的な基準としてそうしたアプローチから適切なものを選択することになる。こうした技術的な基準は、従来からマルウェア対策研究に取り組んできた組織・個人にはノウハウとして蓄積されているが、新たに当該分野に参入しようとする者に広く共有されているわけではない。新規参入の障壁を下げ、サイバーセキュリティ分野を活性化させるためには、こうした安全措置となる技術的な基準を明文化し、普及させることが必要である。海外においては、著名なセキュリティ教育機関であるSANS InstituteのFaculty Fellowが、安全なマルウェア解析環境の具体的な構築方法を実務的なガイドとして示している例がある[35]。

ほかにも、サイバーセキュリティ技術には悪用のおそれがあるため、教育においては技術面のみならず、法的・倫理的観点からの指導も不可欠である。セキュリティ教育において法的・倫理的観点でどのようなカリキュラムが必

要かについては、これまでのセキュリティ教育事業においても事例が存在している。一方で、セキュリティ教育を受けた者がサイバー犯罪に手を染めるリスクをおそれすぎると、サイバーセキュリティ分野の活性化に必須となる教育活動が萎縮してしまい、結果としてサイバーセキュリティ人材の不足にもつながりかねない。サイバーセキュリティ教育の裾野拡大に向けて、教育を実施する大学・研究機関・教育事業者等の間で、必要な法的・倫理的教育内容をカリキュラムの基準として共有することが必要である。

サイバーセキュリティ研究・開発及び教育への参入障壁を下げ、より安全な研究環境を確保するためには、上記のような基準や配慮事項といった知見を蓄積し、研究者が必要なときにいつでも参照できる体制を整えることが不可欠である。

４　まとめ

現代社会の基盤を支える情報システムの分散化・相互接続化に伴い、防御側が攻撃者の思考を先回りする「踏み込んだ研究」が不可欠となっている。一方で、こうした研究活動の実施には、現行法令の解釈の不明確さ、研究成果の公開に伴う社会的影響の大きさ、教育の場における倫理指導の難しさなど、法的・倫理的観点からの課題が多数存在している。

第２章では、これらの課題を具体的事例と共に整理し、研究者・教育者・開発者が直面する現実的な困難を示した。不正アクセス禁止法や不正指令電磁的記録に関する罪に代表される国内法は、今日の研究活動における正当な目的と悪意ある行為の線引きを必ずしも明確にしていない。脆弱性に関する情報の取り扱いに関しては、ISO/IEC 29147 等の国際規格が存在するものの、個別の調整実務までを律するものではない。一方、わが国では「情報セキュリティ早期警戒パートナーシップ」において、関係者間の脆弱性情報の流通と調整が行われているが、限られたリソースのために調整プロセスが長引き、研究成果の公開が遅れる場合があるといった課題も残されている。さらに、若年層の関与を含むサイバーセキュリティ事案の多様化は、教育段階における倫理指導の枠組みを再検討する必要性を示している。

第３章では、サイバーセキュリティ分野の研究・開発・教育を健全かつ持続的に発展させるための提案を示した。具体的には、（１）個別事案について相談を受け、助言を行う相談機関の設置、（２）法的・倫理的判断基準を社会的合意の下で策定し維持するための場の整備、（３）すでに事実上の基準が存在する事項についての明文化・普及、の三点について提案を行った。

今日のサイバーセキュリティ分野は、技術動向の変化が極めて速く、攻撃手法やリスクが継続的に進化している。今後も脆弱性の発見、攻撃手法の高度化、AI の悪用など、新たな課題が次々に生じることが確実である[4]。そのため、法的・倫理的基盤の整備は、単に研究者を守るためだけでなく、研究の活性化を通じて社会全体の安全と信頼を確保するための必須要件でもある。

本見解で示した提案は、サイバーセキュリティ分野における研究・開発・教育の活性化に資する一歩にすぎない。しかしながら、多様なステークホルダーによる議論に基づき完成度を高めてこれらの取り組みを進めることで、わが国におけるサイバーセキュリティ研究開発の進展や人材育成が促進され、将来の社会を支える強固で信頼性の高いサイバーセキュリティ基盤の構築に寄与することが期待される。

[4] 2026 年５月には、AI モデルのサイバー攻撃能力を評価する内部試験において、モデルが想定外の方法でインターネットへのアクセスを獲得する事例が発生し、その後７月には第三者のシステムに侵入する事例が発生した[36]。また同年６月には、サイバーセキュリティを含む安全保障上の懸念から、米国政府が一部の AI モデルについて外国籍者によるアクセス停止を求める指令を出し、その結果、当該モデルのサービス提供が停止される事例も生じた[37]。

＜参考文献＞

[1] Patrick Howell O'Neill、サイバー攻撃で病院のシステムが停止、救急患者が死亡＝ドイツ、MIT Technology Review、2020 年 9 月
https://www.technologyreview.jp/s/220021/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/

[2] 情報処理推進機構（IPA)、制御システム関連のサイバーインシデント事例 11、2024 年３月
https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/incident_11_20240417.pdf

[3] 警察庁、不正アクセス行為の禁止等に関する法律の解説、2012 年、
https://www.npa.go.jp/bureau/cyber/pdf/1_kaisetsu.pdf

[4] 法務省、いわゆるコンピュータ・ウイルスに関する罪について、2011 年、
https://www.moj.go.jp/content/001267498.pdf

[5] 高市早苗、サイバーセキュリティ対策④：セキュリティ研究者・技術者の法的保護、2019 年８月 30 日
https://web.archive.org/web/20251021182231/https://www.sanae.gr.jp/column_detail1207.html

[6] 「無限アラート」で女子中学生を補導、「リンク貼り付け」で摘発をどう考えるか、弁護士ドットコムニュース、2019 年３月７日、
https://www.bengo4.com/c_23/n_9333/

[7] アラートループ事件の被疑者２名に対する起訴猶予処分を受けて、弁護人 南竹 要、2019 年５月 29 日、https://calamvs-law.site/wp-content/uploads/2023/03/%E5%A3%B0%E6%98%8E%E6%96%87.pdf

[8] 最高裁判所 第一小法廷判決、2022（令和４）年１月 20 日（令和 2(あ)457)、
https://www.courts.go.jp/hanrei/90869/detail2/index.html

[9] セキュリティ会社の社員逮捕、ウイルス拡散が疑われるも残る疑問、日経 XTECH, 2017 年 11 月 20 日、
https://xtech.nikkei.com/it/atcl/column/14/346926/111701209/

[10] 「何がセーフか分からない」ウイルス罪で罰金刑を受けた技術者の嘆き、日経 XTECH、2019 年４月 24 日、
https://xtech.nikkei.com/atcl/nxt/column/18/00722/042200002/

[11] Librahack、容疑者から見た岡崎図書館事件、http://librahack.jp/

[12] 東京地方裁判所判決、2024（令和６）年９月 26 日（令和 6(行ウ)121)

[13] 文化庁、著作権法の一部を改正する法律（平成 30 年法律第 30 号）について、2018 年、
https://www.bunka.go.jp/seisaku/chosakuken/hokaisei/h30_hokaisei/

[14] Electronic Frontier Foundation, ″US v. ElcomSoft Sklyarov″,

https://www.eff.org/cases/us-v-elcomsoft-sklyarov
[15] Wikipedia, "DeCSS", https://en.wikipedia.org/w/index.php?title=DeCSS&oldid=1337864460 , 2026 年 2 月（本件に関する情報は多岐にわたり分散しているが、各種情報源がこのページにまとめられている）
[16] "Supplement to the Proceedings of the 22nd USENIX Security Symposium", USENIX Association, Aug. 2013, https://www.usenix.org/sites/default/files/sec15_supplement.pdf
[17] "MBTA v. Anderson: D. Mass: MIT Students' Security Presentation Merits Temporary Restraining Order", Jon Choate (edited by Dan Ray), Harvard Journal of Law and Technology (JOLT) Digest, August 2008, https://jolt.law.harvard.edu/digest/mbta-v-anderson
[18] 世界医師会（WMA）日本医師会訳、世界医師会ヘルシンキ宣言 人間の参加者を含む医学研究のための倫理的原則、2024 年改訂、https://www.med.or.jp/doctor/international/wma/helsinki.html
[19] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, The Belmont Report. Washington, DC: United States Government Printing Office, Sep. 1979, https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html
[20] US Dept. of Homeland Security, The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research , Aug. 2012, https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf
[21] Harshini Sri Ramulu, Helen Schmitt, Bogdan Rerich, Rachel Gonzalez Rodriguez, Tadayoshi Kohno, Yasemin Acar [Extended] Ethics in Computer Security Research: A Data-Driven Assessment of the Past, the Present, and the Possible Future, CCS ' 25, October 13-17, 2025, Taipei, Taiwan, https://doi.org/10.48550/arXiv.2509.09351
[22] 秋山満昭、島岡政基、サイバーセキュリティ研究における倫理的配慮のサポート、情報処理 61(4)、378-383、2020 年 4 月
[23] Robert B. Ramirez, Tomohiko Yano, Masaki Shimaoka, Kenichi Magata, Knowledge-Base Practicality for Cybersecurity Research Ethics Evaluation, Computer Security Symposium 2020
[24] Tadayoshi Kohno, Yasemin Acar, Wulf Loh, "Ethical Frameworks and Computer Security Trolley Problems: Foundations for Conversations," 32nd USENIX Security Symposium, 2023, pp. 5145-5162.
[25] IEEE S&P'21 Program Committee, "IEEE S&P'21 Program Committee

Statement Regarding The “Hypocrite Commits” Paper,″ May 2021, https://www.ieee-security.org/TC/SP2021/downloads/2021_PC_Statement.pdf
[26] CSS2021 研究倫理相談 TF/MWS/OWS/UWS 連携企画、Hypocrite Commits 論文から考えるサイバーセキュリティ研究倫理、2021 年 10 月 27 日、https://www.iwsec.org/mws/2021/ethics20211027.html
[27] USENIX Association, ″USENIX Security ’26 Call for Papers (Ethics Guidelines)″, https://www.usenix.org/conference/usenixsecurity26/call-for-papers （2025 年 11 月 30 日閲覧）
[28] 情報通信研究機構ナショナルサイバートレーニングセンター、SecHack365 における法律と倫理に関する教育について、2023 年 9 月 12 日、https://sechack365.nict.go.jp/news/20230912.html
[29] 井上トシユキ、「3 分で 7 万 5000 円」中学生ら不正アクセスによる転売で逮捕　大手携帯会社の厳重セキュリティ突破した“手口”の裏側とは、弁護士 JP ニュース、2025 年 3 月 4 日、https://www.ben54.jp/news/2009
[30] サイバーセキュリティ情報局、「モリスワーム」がこの世にもたらしたもの、2017 年 3 月 1 日、https://eset-info.canon-its.jp/malware_info/trend/detail/170301.html
[31] 厚生労働省、ICH E8(R1) 臨床試験の一般指針、2022 年 12 月 23 日、https://www.pmda.go.jp/files/000250244.pdf
[32] マルウェア対策研究人材育成ワークショップ、サイバーセキュリティ研究における倫理的な研究プロセスについて、https://www.iwsec.org/mws/ethics.html
[33] Stephen Shepherd, ″How do we define Responsible Disclosure?,″ SANS Institute, Feb. 2003, https://www.sans.org/white-papers/932
[34] Digital Millennium Copyright Act, Public Law No. 105-304, 112 Stat. 2860, 1998.
[35] Lenny Zeltser, 5 Steps to Building a Malware Analysis Toolkit Using Free Tools, zeltser.com, Jan. 2010 (updated Jan. 2021), https://zeltser.com/build-malware-analysis-toolkit
[36] OpenAI, ″The Hugging Face incident and the road ahead,″ Aug. 2026, https://openai.com/index/hugging-face-incident-and-the-road-ahead/
[37] Anthropic, ″Statement on the US government directive to suspend access to Fable 5 and Mythos 5,″ Jun. 2026, https://www.anthropic.com/news/fable-mythos-access

＜参考資料１＞審議経過

2024 年

10 月８日　サイバーセキュリティ分科会（第１回）
役員の選出、今後の分科会活動について

12 月 17 日　サイバーセキュリティ分科会（第２回）
話題提供と議論、今後の分科会活動について

2025 年

３月３日　サイバーセキュリティ分科会（第３回）
話題提供、見解作成に向けて

５月 15 日　サイバーセキュリティ分科会（第４回）
話題提供、見解作成に向けて

９月 18 日　サイバーセキュリティ分科会（第５回）
見解作成に向けて

2026 年

１月 21 日　サイバーセキュリティ分科会（第６回）
見解の発出に向けて