CSS2018 企画セッション「サイバーセキュリティ研究のグレーゾーン」の報告

実施日時：2018 年 10 月 24 日（10:35 - 11:55）
企画概要：
サイバー技術を扱うことは，技術者による様々なサイバー事件にもあるように， 思わぬ事態を引き起こすことがある．特に，サイバー技術を使う研究活動・技術開発をする上で， どのような行為が社会に取って好ましくないのかが立場によって解釈に違いが見られることもある． また，その一方，研究開発コミュニティへの萎縮を招くことがあるとなると，我が国の研究開発自体への悪影響も予想される．本セッションでは，あまりオープンに議論されることがない， 特にサイバーセキュリティ技術・研究のグレーゾーンについて，法曹関係者も含めた有識者による講演と パネル討論を通じて，多面的に現状と今後について議論する．
モデレータ：
寺田 真敏（日立製作所）
パネリスト：
北條 孝佳（西村あさひ法律事務所）
高木 浩光（産業技術総合研究所）
吉峯 耕平（田辺総合法律事務所）
吉岡 克成（横浜国立大学）

―――以下，当日の講演・発言のまとめ―――
【サイバーセキュリティのグレーゾーン・研究倫理について】
モデレータの寺田真敏氏（以下，寺田氏）より，簡単に背景の説明（スライド 0 の P3～5 参照）の後，パネリストから，サイバーセキュリティのグレーゾーン・研究倫理について，それぞれの立場から 10 分ずつ講演をしてもらった．

北條佳孝氏（以下，北條氏）から，サイバーセキュリティを研究するためには，サイバー攻撃そのものを知る必要があるが，攻撃を知るために試す行為自体が犯罪に該当する可能性があるとの考えが示された（スライド 1 参照）．
＜以下，北條氏の発言のまとめ＞
- 海外の事例として，シンガポールでのサイバーセキュリティ競技会に参加した中国人エンジニアが，宿泊していたホ

テルの WiFi の脆弱性を発見し，この内容をブログに公開したことで，約 40 万円の罰金刑を受けた.

- 別の例として，ハニーポットの研究においては，研究者自身が用意したハニーポットを攻撃させて踏み台となる状況を放置することや，攻撃者にビーコンあるいはウイルスを埋め込んだファイルを持って行かせて開かせることにより，攻撃者の IP アドレスを取得したり，ウイルスに感染させたりする行為は，不正指令電磁的記録作成等罪に抵触する可能性がある
- 脆弱性を発見する行為自体・目的自体はさておき，該当するソフトウェア等の開発元に無断で公開してしまう行為は問題である.
- 学術研究の場合は，各種除外規定のある法律も存在するがどこまでが研究として許されるかは知っておくべきである

高木浩光氏（以下，高木氏）から，高木氏の過去の経験より，いくつかの事例等が紹介された（スライド 2 参照）.

＜以下，高木氏の発言のまとめ＞

- 2000 年頃は，脆弱性が発見された場合の対処のあり方が社会に理解されていなかった．たとえば，Java 実行環境の脆弱性を利用すると Web サイト上のアプレットで PC のローカルファイルが読めるというケースでは，当時，なにが問題なのかがわからない人が多かった．そのため，（問題であることを知らしめるために，高木氏が）実演を通して，この脆弱性問題を知らしめた.
- これが Web アプリの脆弱性の場合には，実演することは，サーバ管理者の意思に反するので，不正アクセス禁止法にあたるのではないかという意見もあった
- 2002 年には，ディレクトリ一覧によりファイルが露出する Web サイトが数多くあり，この露出したファイルを暴露する行為が横行し，これが不正アクセスだという意見もあった．しかし，警察庁が，これは道端に資料を置いているのと同じだ，不正アクセス禁止法のカバーする範囲ではないとコメントしたことにより，その行為がさらに横行して被害が続出したが 1 年くらいで収束した．もし，これを違法行為として取り締まっていたなら，皆が見て見ぬ振りする社会になっていただろう
- 問題意識が低い中で，社会に対して問題の所在の明らかにして行くという大きな目的のためには，なにかしら大きなことをしないと解決しないという面が見えた
- 一方，2005 年の ACCS（Association of Copyright for Computer Software，コンピュータソフトウェア著作権協会）事件では，脆弱性（ディレクトリトラバーサル）を突く実演により，閲覧できてはいけないものを画面に出した．これが刑事事件となり有罪判決となった
- こういったこともあり，公的機関が仲介すべきじゃないのかということで，IPA に脆弱性届出制度ができた．IPA のサイトには，脆弱性の発見をする上での留意事項が掲載されている
- 不正アクセス禁止法は，形式にやってはいけないことを法律として定めただけであり，実害のあるなしは関係ない．実害があってもルールに違反してなければ刑法上は違法でない場合もある．脆弱性届出制度も，問題のない範囲で脆弱性を発見する手法（寸止め）のノウハウが蓄積されていった
- 2014 年，雑誌社とセキュリティベンダが上場企業 100 社と府省庁に無断で脆弱性診断したが，大きな問題にまでは発展しなかった．この 10 年の間に社会の考え方が変わったと考えられる．ある範囲であれば，脆弱性のテストはやっても良いという世論になった様子がある
- 2018 年の Coinhive 設置者検挙事件については，類似の事例として米国で MIT の学生が Bitcoin で類似

のものを作り，ニュージャージー州消費者詐欺防止法に違反するとして州の司法当局の調査が入ったが，EFF(Electronic Frontier Foundation，電子フロンティア財団)が助けに入って和解に至った事案がある．その一方で，日本では，（Coinhive 設置者検挙事件について）警察庁の「社会的なコンセンサスがない」とのコメントがテレビで放送されたが，「社会的コンセンサスはいつできるのか？」「社会的コンセンサスがないうちには研究はできないのか？」という論点が上がってくるだろう

吉峯耕平氏（以下，吉峯氏）から，医学研究の場面で同じようなところがあるのではないかという観点より，事例等が紹介された（スライド 3 参照）．

＜以下，吉峯氏の発言のまとめ＞

- 倫理的な問題とは，「絶対に正しい答え」はないことを倫理的な問題として捉えている
- （医療の現場では）延命治療を中止するのかなどの終末期医療は何が正しいのかをケースバイケースで議論する，それを法律で書くことは困難である．医学研究（人体実験）をやって，薬・治療は効果があるかどうかを確認して，皆が利益を得る．効くかわからない薬を試してよいのか？新薬の効果を確かめるために，プラシボ（偽薬）を投与はよいのか？といった倫理的な問題があるが，実施する必要はある
- 医学研究では（倫理的なケアを）どのようにしているのかというと，大きく分けて，手続き的ルールと実体的ルールがある．手続的なルールには，「研究計画書の作成」「倫理審査委員会の審査を受ける」があり，実体的なルールには，「インフォームドコンセントの実施」がある．この 3 つを踏まえた（スライド 3 の P.5 参照）プロセスを踏まないと論文が発表できないこともある
- なぜ，このようなプロセスができたのかの原点は，ナチスの人体実験の歴史にあり，その反省から世界医師会がヘルシンキ宣言を出し，これが大きな枠組みとなっている．さらに，1960 年代米国でのタスキギー事件でも，経済的弱者が犠牲になった．他にも類似事件があった．これらを受けて院内審査委員会（IRB）が義務化（1974）され，さらに，ベルモント・レポート（1979）につながった
- なぜ，このようなルールの必要性があるのか？というと，「医学研究」は「医療」と違うからである．観察研究より介入研究は，（倫理的なケアについて）厳密にやる必要がある．それは，「将来の患者の利益」と「現在の患者のリスク」をどのようにバランスするのかという問題意識があるからである
- さらに，ルールを整備することで研究者個人を守られていることもある．川崎協同病院事件（終末期医療）にもあるように，個人・独断で実施すると問題となる．（個人で勝手にやらずに）議論して組織として議論しましょうということが重要であると言える．組織・コミュニティに自主的なルールがないと問題が発生した場合，それが流石に無視できないとなると刑法の適用に繋がる可能性がある．よって，自主的ルールはコミュニティ・個人を守るために必要である．医療もサイバーも同じであると考えられる

吉岡克成氏（以下，吉岡氏）から，研究者の立場から，「CSS2018 研究倫理委員会」「その経験を踏まえてやるべきこと」「法執行機関と上手く付き合って成果がでた事例紹介」の 3 点について示された（スライド 4 参照）．

＜以下，吉岡氏の発言のまとめ＞

- 背景として，「新たな攻撃手法、脆弱性の発表」，「実運用中のシステムに影響のある実験」「被験者に危害が及ぶ可能性のある実験」などが，CSS や CSEC（Computer Security Group，情報処理学会 コンピュータセキュリティ研究会）のみならず，世界的なトレンドであり，トップカンファレンスでも攻撃系の研究が増えてきた
- そのような背景の中，「研究成果が悪用される恐れはないか？」「実験が人・システムに危害を与えていないか？」

「この研究はやってよいのか?」という疑問が持ち上がる．そこで，CSS2018 では，「研究倫理委員会」および「相談窓口」を設置した（スライド 4 参照の P.4）．危害より恩恵が大きい場合をよしとするというメンロレポートの考え方をベースに，研究の正当性を判断した．ここで，メンロレポートとは，ベルモントレポートの 3 原則に，さらに 1 原則（「法と公益の尊重(Respect for Law and Public Interest)」）を追加し，4 原則を定めている

- 「相談窓口」では，投稿前の相談を 4 件（スライド 4 の P10 参照）受けた．6 名体制で 5 営業日くらいで対応した．倫理プロセスの普及活動もあり，研究倫理について触れている論文数が増えてきている．また，どうすればインパクトがある研究になるかなど前向きな議論となった
- 「投稿論文倫理チェック」では，投稿後プログラム委員会からの指摘された論文への対応であり，全部で 4 件あった．いずれも「脆弱性の開示方法」いわゆる Responsible Disclosure に関する指摘であった．こちらは，チェックする側もされる側も大変であるが，研究コミュニティとして向き合わなければいけない問題でもあると認識している
- 最後に，法執行機関と上手に付き合って成果を出した例の紹介があった（スライド 4 の P16, 17 参照）．この研究では，お金払って DoS を打つ実験行為を実際に自分たちの観測環境に行い攻撃を詳細分析していた．この研究手法が，法的グレーゾーンと著者らも認識していたが，最終的に恩恵が大きいと判断している

【意識しなければならない倫理プロセスについて】

次に，フリーディスカッションとして，モデレータの寺田氏より，「研究開発コミュニティが萎縮しないために ～意識しなければならない倫理プロセス～」について，パネリストから意見を貰うことになった（スライド 0 の P.6 参照）．

北條氏：

- 研究行為が法律に抵触するのか否かの指導は担当の先生や，研究指導者がすべきである
- 法律等に詳しくない先生方もいるかもしれないが，先生方も法律等を学ぶべきである．
- 新しい法律やその立法過程，解釈，裁判例，過去に発生した事例や事件を知っておくべきである

高木氏：

- 平凡な研究をするのであれば第三者に頼るのもあるが，相談すると「できない」という方向になる．特に，組織的な対応をするほどそうなる
- 最先端で何かを解決しようとするとき，特に突出した研究のときには，先生・研究者が自分で考える必要がある．結局，研究の社会的必要性を理解していないと（倫理的な判断をするのは）難しい
- 医療は生命・身体に関わるので重い審査プロセスを回す必要性があるが，IT など変化していく世界で重い審査プロセスが回るのかは疑問がある
- （CSS2018 の取り組みについて）「発表して良いのか」は当事者に考えて貰うしかない
- 脆弱性届出制度ができたことで，研究者の間にすべて届けないといけないという風潮が一時広がったが，この制度は，個々の製品及びウェブサイトを扱う場と整理された．暗号やプロトコル等はこの制度で扱わず，学会で扱われることが期待されている

吉峯氏：

- 刑事事件になっている時点で手遅れである．裁判例・判例はある意味事後事例であり，すでに手遅れである

- 裁判では，検察官の主張が判断に強く影響しており，弁護人の立場としては非常に不利である．検察側が起訴したことを無罪とするのは非常に難しいので，なるべく起訴になる前の段階で処理していくことを試行するのがよい
- 裁判例を勉強することで裁判に勝つというのは，法律専門家にとってそれで良いかもしれないが，裁判にならないように適切に研究を進めて公益に資すると言う観点からはそれでは足りない
- 弁護士が相談されればリスクがあると答えるが，それは（研究者には）何の役にも立たない．コミュニティの中に法律家も入って一緒に考えていく・議論をしないといけない
- 弁護士も継続的な活動をするためには，その（経済的・制度的な）仕組みが必要
- 医療でも病院ごとに倫理委員会を擁しているが，皆が詳しいわけではない・形骸化の批判もあるが集合知で対処すべきである
- 終末期医療のケースでは，国の前に，学会から自主的にガイドラインを用意した．学会で議論して，学者コミュニティのコンセンサスを作らないと学問の自由というのは確保できない

吉岡氏：

- CSS（MWS）では，（吉岡氏や）秋山満昭氏(NTT セキュアプラットフォーム研究所)らが継続的に倫理プロセスの普及活動を活動している
- メンロレポートの翻訳など用意して勉強する土台を作っており，それらの資料が，MWS のサイトでまとめられ，誰でも見られるようになっている
- サイバー研究の倫理問題は 2 つあると思う：ハイエンドとローエンド
- ハイエンドは自分で判断するしかない．自分達で考える必要がある．また，その手のことをしている人は，しっかり（倫理的ケアを）やっていることを論文の中に書いている．問題になったときの準備・論理武装をしている．ただし，一人で考えられないのも事実であり，議論の場はあった方が良い
- ローエンドは，チェックリストみたいなものが効果あるのでは？ 周知を徹底して，うまく気づいて貰う仕組みが必要

【最近気になった事例について】

寺田氏より，最近の事例（セキュリティ会社社員逮捕事件，仮想通貨マイニングスクリプト設置者検挙事件）について，パネリストに質問があった．

北條氏：

セキュリティ会社事件：

- セキュリティ企業でもやっていいことといけないことがある．また，セキュリティ企業として自社のシステムについてどこまで把握していたのかという疑問がある

仮想通貨マイニングスクリプト設置者検挙事件：

- マイニングスクリプト頒布事件の件については，「意図に反する」と「不正な」の 2 つの解釈が問題になる．「意図に反する」と「不正な」の解釈について，色々な解釈が飛び交っており，明確な解釈とはいえないことが心配なのだろう．ただ，過去に，立法担当者などが解釈を提供しているので参考になる
- 基礎的な土台，基礎的な事例・判例・法律を知ることがまず重要である．知ることをしないで，感情論とか，技

術を阻害するのでこれダメじゃないというのは，ちょっと違うのではないか

高木氏：

セキュリティ会社事件：

- （不正指令電磁的記録の）保管罪で検挙と報じられたため，被疑事実が何かを誤解して不当な検挙だとの批判が一部に見られたが，実際はファイル共有ソフトで共有状態を続けた事案であり，供用未遂罪に当たり得るものだった．グレーゾーンの議論には当たらない

仮想通貨マイニングスクリプト設置者検挙事件：

- 裁判が始まっており，不正指令電磁的記録罪の「意図に反する」「不正な」の解釈が争点になると思われる
- 不正アクセス罪と比較してみると，そちらは人工的なルールであり，法定犯・行政犯に分類されるもので，実害がなかろうがルールを破れば違法である．たとえば，複数の記者が報道目的で犯罪者のパスワードを推測してウェブメールにログインして記事にしたところ，書類送検されて起訴猶予となった事案がある．不正アクセス禁止法は，保護法益に立ち戻ると，立法の経緯や目的条項に書かれているように、アクセス制御機能の社会的な信頼を保護するものであり，記者らの行為はこれを害したということ
- これに対し，不正指令電磁的記録罪は，刑法典に列挙されていることから，自然犯と言うべきものだと考える．（2011 年の刑法改正は）本来的に悪い人を捕まえるための理由を追加したに過ぎず，不正アクセス禁止法のように行政的にルールを追加したのとは異なる．ウェブマイニングは迷惑行為かもしれないが，法の条文に形式的に当てはまるからなどという理由で刑法典の犯罪として扱うのは何かを間違えていると思う
- 当時(2011 年)は国会で自分も法案に賛成したが，不正指令電磁的記録罪は失敗作だったと思う．「意図に反する動作させる」「不正な指令」は，電子計算機損壊等業務妨害罪(1987 年)にも現れるフレーズだが，そちらの場合は，「人の業務を妨害」に結びついており，解釈が限定的であったが，不正指令電磁的記録罪の場合は，「人の業務を妨害」が取れたことで宙ぶらりんの，限定のない裸の要件となってしまっており，この立法の失敗を法学研究として批判していきたい

吉峯氏：

- 刑法の謙抑性ということを考えたい．悪気があった人はあまりいないと思われる．その行為により，警察のお世話になるとは思っていた人はないと思われる
- 刑法の適用というのは非常に峻烈であるので，（吉峯氏自身は）身柄拘束しないで（捜査を）やるべきとの主張をしており，そうなってきたとみているが，捜索差押えは市民にはショックが大きいことを考えないといけない．これらが刑法犯に当たるのだと事前に知らされていれば，みんなやらなかったのではないか．住居侵入などであれば一般市民がだいたいわかるが，仮想通貨マイニングスクリプト設置者検挙事件は過度に厳しかったのではないか
- 同意を取れば良いという反論があるが，利用規約に書けばよかったものがウイルス的なものと言えるのか？もっとマイルドな規制手段があったのではないか？

吉岡氏：

- 感想として，すごくショックを受けた
- セキュリティ会社でも間違いが起こることを見て，大学ではハニーポットの運用とかを学生にさせることは非常に危ないという印象であり，厳しく指導するしかないと考える

- 誰に聞いてもわからない，法解釈もわからないので困っている

【フロアからのコメント・質問】

高倉弘喜氏（国立情報学研究所）：

- 海外では（研究倫理について）議論が活性化しているので，日本でも行われていることはありがたい．ただし，誰が判断するのか？となると難しい．最終的には研究機関で判断してくださいだと思うがいきなり研究機関に降るとネガティブな反応が来るのが見えている
- なので，このような場で学会の方針を示すことが重要である
- 議論をして方向性を決めて欲しい．あまり時間がないのでは？

篠田陽一氏（北陸先端科学技術大学院大学）：

- 倫理プロセスを確立して行く・積み上げて行くことが大事．それによって，警察などが来ても，反論できうる
- タイムリミットはなく，（研究者が）ドキドキすることではない．それよりも，横幅・スペクトラムが広がっている
- （CSS といった場所は）チェックプロセスのような（論文を）通す・通さないではなく，教育的な土壌を作る場であるべきである
- サイバー研究も，工学における実験法・お作法を確立して，周知していくべきだろう

松浦幹太氏（東京大学）：

- 情報セキュリティに特有の問題として，簡単に国境を越えるという点がある
- 人材育成の観点での議論も大事だろう
- 工学部 4 年生の講義で使う予定で執筆した教科書の 1 セクションで，倫理を取りあげている．基礎講義だけで解決はできないが，問題から目をそらしてはいけない
- こういう場に学生が参加しやすいようにして欲しい

【企画セッションを締めくくるにあたって】

寺田氏より，パネリストに対して企画セッションを締めくくるにあたり，「研究開発コミュニティが萎縮しないために」を踏まえたコメントが求められると共に、「サイバーセキュリティ研究のグレーゾーン」の問題については，会場にいる皆も一緒になって，今後も取り組んでいくことで，企画セッションを締めくくった。

北條氏：

サイバーセキュリティが医療と大きく違うのは，年配でも若者でも誰でも，どこにいても家であっても実践できてしまうことである．家にいてネットワークがつながっていれば，外部への攻撃もできてしまう．どのようなことが悪いことなのか，してはいけないのか，法律に抵触するのかといったことを誰も教えてくれないし，誰に聞いたら良いのか分からない，そのような状況が非常に問題になっている。学校でも職場でもサイバーセキュリティに関する法律や事件，事例を教える場が必要なのではないだろうか．

研究内容がグレーであり先生方でも判断できない場合は，大学以外でも良いので，相談できる窓口を設けるようにす

るのがよい．窓口は一時的なものではなく，常時設置しておくべきであろう．

高木氏：

今日は，刑法の話がたくさん出たが，民事上の損害賠償を求められることもありうる．相談するとやめておこうかということになりがちだが，研究としてやるべきものであれば，賠償覚悟でやることはアリであろう．

個人情報保護法や EU の GDPR に触れるような個人データを扱う研究も，学術研究の適用除外があるが，法の趣旨は踏まえよということになっている．しかし，「こういうことをやると社会的に問題なるよ」と先に実演してみせるという研究もありうるわけで，予防的に「被害」を軽く出して示すこともアリだろう．刑法だけでなくいろんな面から考えないといけない．

（篠田先生への回答として）今日は，「無頓着にやっている人がいる」「ルールがありますよ」「でも過剰に反応しないでくださいね」という話が出たが，それも時代とともに変わっていく面があるだろう．つまり，サイバーの分野も今は過渡期であるので過激な研究もあるが，今必要とされているだけで，将来，その必要性が変わっているかもしれない．時代の変わり目を敏感に感じ取ってもらいたい．

吉峯氏：

国を頼るな，国からのお墨付きを期待するなと言いたい．

「医学研究はいいね」と見えたかもしれないが，指針の乱立であり，大混乱の歴史（スライド３参照）である．（乱立した指針を）理解できる人はあまりいないだろう．また，役所がやることというのは前例踏襲であり，ルールを作ってもらうとなる大変なことになる．学会などにおいて自主的にガイドラインを作ることが大事であろう．

医療業界でもお墨付きが欲しいと願ったがそれは難しい．役所は自分たちを縛る個別具体的なことは言わない．しかしながら，自主ガイドラインができて，概ねそれに則って運用されてから大きな問題に発展した例はない．

（サイバー研究者も）「自主的にガイドラインを作り運用している」，「リスクをとってやっている」ということが適正と認められれば，（行為の正当性は）認められていくであろう．

吉岡氏：

今日の議論だけでも，高度な先端から明らかな失敗談と多様であり，これを一つの研究倫理とするのはよくわからないものになる．（自分としては）分解能を高めて，できることからやっていきたい．そうは言っても，「個別具体的に先端研究者が集まって議論しないとできないのではないか」，また，「相談する場，議論する場を，無理ない形でどう作るのかが大事だ」と感じた．

厳しい競争の中で，サイバーの研究者はギリギリでやっており，どう倫理的にやっていくかは非常に難しく，議論をする場をどのように作るかは課題である．CSS 倫理委員会の活動やこのような活動は，何かしらの形で公開していきたい．

以上