資料１－３

サイバー（フィジカル）セキュリティと刑事立法学

千葉大学　西貝吉晃

〔情報化社会におけるにおけるサイクル〕

①技術の進歩⇒新しいソフト、IoT（CPS、サイバーフィジカルシステム）の開発・提供・利用・普及⇒②プログラムに内在する脆弱性の発見に基づく新たなサイバー攻撃の発生・激化⇒③セキュリティ・ホールを塞ぐ等の技術的対応＋刑事罰等での法的対応⇒　①技術の進歩　に戻る

1．サイバーセキュリティと刑事立法学

【骨子】立法時では未知の犯罪行為に対応するための立法方法論が必要になるところ、積極的な違法性阻却の適用を前提とする、ある程度、包括的な構成要件を作ることを提案したい。

(1)　新たなサイバー攻撃に対応するために、ある程度包括的な構成要件が必要になり得ること

未知の行為態様を捕捉できるような構成要件を作る必要がある。

しかし、広すぎると、サイクルプロセス①に対する萎縮効果が大となる。

例 1(サイバーセキュリティの侵害に直接関連する規定の場合) : コインハイブ事件で問題となった不正指令電磁的記録に関する罪については 1. を考慮したとしても、保護法益（プログラムの動作に対する信頼）及び構成要件が広くとられ過ぎたと考えており、いわゆるサイバーセキュリティの保護以上の保護を提供することで、「セキュリティに詳しい人」がみても、どの範囲までのプログラムが捕捉されるか、判別しにくい。（後掲文献イ、ウ）

例 2(サイバー空間の存在により法益侵害が激化し得る場合) : 刑法 175 条のわいせつ罪については、平成 23 年改正前はわいせつ「物」のみが客体であり、データは客体でなかったので、データを直接に捕捉することは出来なかった（データを捕捉する裁判例はあったが、異論は強く、結局、刑法改正によって刑法 175 条 1 項後段が入れられることになった)。情報の伝達という観点からは、刑法 174 条との関係も意識しつつ、より広く構成要件を作ることも立法論としては考えられる。

(2)　新たなサイバー攻撃に対応する過程で、ある程度包括的に違法阻却「も」考えるべきこと

(1)で、ある程度包括的な構成要件を設定する場合、具体的な事情に応じて、ある程度包括的に違法阻却を考える必要が出てき得る。既に、通信の秘密侵害罪のような包括的な構成要件については、ISP の業務として必要な行為については違法阻却が行政解釈で提示されることもある。

なお、セキュリティ業者は、研究目的でマルウェアを保管、実行等する必要があり得る。不正指令電磁的記録に関する罪の広い構成要件に該当しても、違法阻却を広く捉えるべき余地があり得る。

(3)　構成要件を広く作ってしまった場合の救済は？

立法の失敗などと嘆く必要はない（完璧主義からの脱却)。むしろ、立法の試行錯誤もサイバーセキュリティ維持向上のために必要。個別の事案をみて、事案の軽微性を理由に違法性を阻却する（可罰的違法性を阻却する）ことも積極的に考えつつ、場合によっては、新しい事案類型の捕捉の可否も含めた法改正を行う（立法過程での PDCA サイクル)。

2．サイバーフィジカルセキュリティと刑事立法学

(1)　現状の観察

サイバー犯罪とフィジカルな世界での犯罪がまるでパラレルワールドのように別に規定されているのが、基本的な刑法体系の現状である。

イメージ：

私文書偽造　と　電磁的記録不正作出

住居侵入　　と　不正アクセス（発表者は対応しているとは考えていないが･･･）

詐欺　　と　電子計算機使用詐欺

しかし、IoT、CPS に対するサイバー攻撃は、広範囲に物理的な被害をもたらすだけでなく、多数の生命侵害（病院で管理しているデータの改変等（ランサムウェア））等をもたらす可能性がある。重要インフラの保護は最大限図る必要があり、刑事立法をこの文脈で考える場合には、サイバー攻撃からフィジカル侵害へのつながりを意識した立法が求められる。

(2)　2 方向からのアプローチ（挟み撃ち的立法）

①フィジカル侵害についての犯罪（公共危険犯等）の処罰を「ハッキングレベル(システムへの侵入の段階)」にまで早期化する。ただし、一般の予備罪等を使うべきではなく、サイバー攻撃に行為態様を限定すべきである。

例）重要インフラの重要なコンポーネント（構成要素）に対する無権限の操作を包括的に禁止する。

新幹線特例法上の「みだりに操作罪」のハッキング版等が考えられる。

②サイバー犯罪の結果的加重犯的なものを創設するか

例）電子計算機損壊等業務妨害「致死」罪やその他の公共の危険をもたらした場合に加重類型を新設する（ドイツやオーストリアの立法例が参考になる)。既に公共危険を考慮して立法されているようにみえるものにハイジャック防止法上の運航阻害罪（業務妨害罪の特則であるが 10 年以下の懲役と重い）等がある。

※　参考文献

・一般的なサイバーセキュリティと法律についての文献

技術（アーキテクチャ？）と法律（規制？）の協働によるセキュリティの確保について

ア　拙著『サイバーセキュリティと刑法』(有斐閣、2020)

1.（サイバーセキュリティと刑事立法学）についての参考文献

イ　拙稿「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」法セミ 792 号 40 頁(2020)

ウ　拙稿「不正指令電磁的記録に対する罪の解釈論」罪と罰第 58 巻 3 号(2021.6(*to appear*))

2.（サイバーフィジカルセキュリティと刑事立法学）についての参考文献

エ　拙稿「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(2019)

オ　拙稿「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(2021.6(*to appear*))　…　制御システムのセキュリティから航空や道路といった交通から、電気・ガス・水道までの我が国のインフラ保護立法の現状を俯瞰。継続して研究。

以上