資料２－２

デジタル時代の刑事法の在り方に関する議論の整理

０．背景

規制改革推進会議成長戦略ワーキング・グループ（以下、WG という。）にて、「デジタル時代における刑事法の在り方について」というテーマで３回（令和３年４月８日、令和３年４月 27 日、令和３年５月 17 日）にわたり議論をした際の委員及び有識者の意見を整理した。

今後ともデジタル社会の基盤整備という観点から刑事法の在り方について適時適切に議論していくべきである。

１．はじめに

デジタル技術の進展は、ビジネスや働き方、生活習慣などあらゆる分野で大きな変化を生み出しつつある。一方、デジタル技術が、家電や自動車、工場など様々な場面で重要技術として活用されるようになり、サイバー空間の脅威は、人の安全や生命にも直結するような、身近なものになってきている。新たな攻撃に対しては、技術面で万全の対応をしていく必要があることはいうまでもないが、技術だけでなく、技術と法規制の双方の観点から抑えていく必要がある。

このためには、刑事法の在り方を議論することは避けて通れない。「デジタル時代の規制・制度について」（令和２年６月２２日規制改革推進会議）では、デジタル技術の進歩が経済社会を大きく変容させる中での民事法や行政法分野における規制制度の在り方を中心に取り上げたところであり、ここでは、その考え方をさらに拡張し、刑事法等制裁面での扱いを検討するものである

経済活動は法制度・政策と密接な関係があるところ、刑事政策もその例外ではない。経済活動が急速にデジタル化されるなか、国民社会生活の安全・安心を確保しながら、デジタル化の流れの中で現行の法制度・政策の見直しを進めていく必要がある。

２．Society5.0 時代に出現する身近な脅威

急速な進歩がみられるデジタル技術を利用した未知の攻撃が現実社会に脅威を及ぼす可能性が出現している。専門家や関係者の間では具体的な脅威の認識が共有されている攻撃類型もみられる。

デジタル技術による現実社会への攻撃は、伝統的な物理空間内での攻撃やサイバー空間内での攻撃以上に、広範囲で甚大な被害を招来するおそれをはらんでいることを認識する必要がある（サイバー（電子）とフィジカル（物理）が融合する Society5.0 時代にあっては、

サイバー・セキュリティを高めるという発想だけでなく、サイバー・フィジカル・セキュリティを高めるという発想も重要である)。

Society5.0 時代では、甚大な法益侵害がいきなり生じる可能性も高く、こうした法益侵害をみすみす許さないようにするためには具体的事件が生じる前に先手の対応の必要性が高いと考えられる。

なお、英国では 2015 年に現実社会に影響を及ぼすコンピュータへの不正行為を処罰する重大犯罪法が制定され、独国では 2020 年に IT セキュリティ２．０法案が閣議決定されており、また、EU では AI 規制案が提案されている。

認証方法に関しては、ID パスワード方式ではない新たな技術が登場している。行動パターンなどから認証する行動認証などがその一例である。音声、指紋認証などと異なり、立ち止まって認証する必要がないことなどが便利な点であり、今後の実用化が期待されている。新たな認証方法が登場すれば新たなリスクも生じ得るだろう。音声認識する IoT 機器にテレビなどの放送を通じて干渉し、誤作動を惹起させる技術なども登場しているところである。

３．デジタル時代における経済と刑事法の関わり

規制の空白や規制による過剰な威嚇力は、商品化に伴う投下資本回復の予測可能性を減退させ、過剰なリスク回避によってイノベーションを阻害するおそれがある。この観点から、刑事法はデジタル時代のイノベーションを支える一翼を担うものであることを再認識する必要がある。

技術の進展が早く、規制環境の変化が早い状況に適切に対応するためには、司法当局・規制当局・技術提供企業間での意思疎通を促進し、状況を総合的に検証した上で、適切な技術的対応と法律的対応とを統合した対応策を迅速にとることができるように体制整備をする（アジャイル・ガバナンス）ことが必要ではないか。

過去にも、技術革新にあわせて規制を導入し、列車運行の安全を図った例として、(東海道) 新幹線鉄道の整備にあわせて制定された「東海道新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法 (現在は「新幹線鉄道における列車運行の安全を妨げる行為の処罰に関する特例法」、以下「新幹線特例法」)」等の例がある。

４．デジタル時代の刑事法の検討体制の在り方について

次々と発展する技術に対応してアンテナを張りつつ、一過性ではなく継続的に議論を進めていくべきである。このためには、刑事司法分野の関係者とデジタル技術の関係者が積極的に意思疎通して、法制度及び法運用を迅速に今日的環境に適合させるよう努力する必要があると考えられる。

５．デジタル時代の刑事法の総論的な考え方の在り方について

（１）体系的整理の促進

既存の犯罪の保護法益を維持しつつ、行為態様を拡充することによりデジタル時代に対応した犯罪類型を創設してきた点は、対象の明確化や実効性、及び刑法の謙抑性の観点から合理的なものとして肯定的に評価できる。

一方で、複数の類型が積み重ねられて複雑化してきた結果、いかなる犯罪が定められているのか、一般人にとって体系的かつ整合的に理解しにくくなってきているとの指摘もある。

また、サイバー空間が、少なくともコンピュータ犯罪立法当時と比較すると、その規模や役割の点で社会的に大きな存在になってきたことから、デジタル関係の犯罪を既存の犯罪に付随した犯罪と捉えることは必ずしも実態を反映していないと思われるに至っているとの議論もある。

今日、デジタル関係の刑事罰につき、所管にとらわれることなく、一括して体系だった整理も必要となるかもしれない。

（２）デジタル時代における構成要件と違法性阻却事由の在り方

①構成要件の在り方

未知の攻撃から法益を守るためには、ある程度、将来を見据えた構成要件を設けることが必要となるが、その場合であっても、構成要件を広くとると萎縮効果が生じ、狭くとると野放図になることに留意する必要がある。今日的な犯罪類型を定める際に特に難題となると思われるその構成要件の書き方については、関係者や技術者との協議を重ね、諸般の状況を考慮にいれつつ、技術者や一般国民にとっての分かりやすさ、予見可能性を重視して、入念に検討を行うべきであることが改めて喚起されるべきではないだろうか。

Society5.0 時代におけるサイバー攻撃は広範囲で甚大な被害を招来するおそれをはらむものであるため、物理的な空間への法益侵害が不正アクセスなど電子的な行為を始める時点で具体的に危険を生じているものとして、危険の判断時点を早期化して捉え、これを危険犯として整備することも一案として考えられる。同時に、サイバー攻撃による重要システムへの侵入については、前述の新幹線特例法をも参照しつつ、これを基本犯とし、結果的に重大な法益侵害を生じた場合に結果的加重犯として処罰する類型を整備することもあり得る。

上記２つは同じ目的を結果からみるか（危険の判断時点の早期化）、行為からみるか（違法行為の結果的加重犯化）の違いであるともいえるが、どのような議論がよいかは、入念に議論する必要があるだろう。

②違法性阻却事由の在り方

罰すべきは罰するという観点（当罰的な行為を犯罪化する観点）とイノベーションを萎縮させてはならないという観点の双方を勘案しつつ、構成要件に該当する行為であっても違法性阻却を広範に認めることで救済するといった発想もあり、こうした意見も否定せずに検討する必要があるだろう。

（参考）有害サイトのブロックと通信の秘密侵害罪の関係やデリバティブ取引と賭博罪の関係などの例があること。これらは、幅広な構成要件を維持しつつ、社会的に相当な行為について広く解釈として違法性阻却される場合を明示した例がある。

③予見可能性の向上

イノベーションを萎縮させる可能性のある犯罪類型については、共犯も含めて、実務の運用に当たり利害関係者や技術者との協議を踏まえ、構成要件の外縁、正当業務行為等の違法性阻却事由の解釈・運用の指針を定めるなど、予見可能性を高める方策を検討することも考えられる。

（３）デジタル時代における構成要件とエンフォースメントの在り方

目覚ましい技術革新の時代には社会的な影響や逮捕・検挙の動向等を見据えつつ、社会の変化がこれまで以上に速いことを踏まえて、これまで以上に迅速に評価、立案を繰り返す不断の検討を行う仕組みが不可欠との議論もある。

構成要件の定め方に関しては、抑止を確実なものとするため、証拠の収集、起訴を見据えて現場が判断しやすいよう配意する立法論が必要であり、引き続きそのような立法を行うことが重要である。

現場が、いかなる証拠を収集し、立証すれば有罪に持ち込めるかが理解できない犯罪類型が設けられることがもしあれば、事実上、犯罪行為が放置されてしまう可能性があり、その状態が続けば「割れ窓理論」により、抑止力が効くどころか逆効果になりかねない。

抑止を確実なものとするためには、犯罪類型を明らかにすることで現場のエンフォースメントが有効に機能する可能性が高いと思われ、特に各省の個別法上の犯罪類型について、特に重要と見られるサイバー犯罪は、現場が適切に理解できるよう明確化していく必要がある。

今後、域外捜査やデータそのものの差押え等の必要性が高くなると思われる中、制度面において適切に対応することも重要であろう。

（４）企業の刑事責任

Society5.0 時代における企業の刑事責任をどのように設計するかは、製品やサービスに関する適切な危険管理のインセンティブを企業に与える上で、重要な意味を持つと思われる。

法人に対する厳格な刑事制裁制度と共に訴追延期合意制度と呼ばれる検察官の訴追裁量を適切に活用するアメリカ合衆国型の制度が英国・ドイツ・フランスを始めとする各国に展開しつつある。

日本においても、これらの先行する諸制度は一考に値すると思われる。その際、日本企業に対する海外当局による法執行が日本のデジタル企業に及ぼしうる影響、日本で活動する海外企業への影響、海外企業と日本企業との公正な競争の実現、日本企業が提供する製品やサービスに対する信頼性や競争力の向上、といった視点も考慮するべきであろう。

６．デジタル時代の刑事法の各論の在り方について

（１）電磁的記録に関する犯罪

電磁的記録を取り巻く社会、技術の環境変化を踏まえれば、電磁的記録に関する処罰の在り方も、今日的状況にあわせて見直すことも考えられる。

電磁的記録においても、制定当時以来の技術の発展に伴い、印章と同様に本人確認機能及び意思担保機能を付すことを可能とする技術が生まれているだけではなく、電磁的記録は、メタデータ等の付随的な情報（いつ、どのように作成したかを記録した情報等）が、データ作成の信頼性を確保する上で貴重な情報と認識されてきている。

民事訴訟やデジタルの専門家との意思疎通を図り、項目毎（例：タイムスタンプ、電子メールのプロパティ欄のアドレス、ワードのメタデータ等）にその重要性の軽重を検討し、反映していく必要もあるかもしれない。同様に、書面に関して印章偽造が処罰対象となるのと同様、電子署名を不正に作出する行為についても何らかの手当を検討する必要があるかもしれない。

さらには、一般人の行動に及ぼす影響を踏まえると、「有印私文書偽造罪」との通称が「有印」の重要性に関し誤解を生じる可能性もあることから、通称の在り方も検討が必要との議論もあるところである。

（２）「みだりに操作」罪（コネクテッドカー）

コネクテッドカーにつき、自動車内部の運転制御装置をハッキングされることを防ぐため、ECU を複層的に設ける構造的な手法を採用した場合であっても、他者が自動車に乗り込み直接最深部の電子計算機を操作する可能性や自車改造により信号機等へのインフラへ干渉する行為などが懸念されているところである。

自動車に乗り込んで最深部の電子計算機を直接操作されると、電子計算機のセキュリティは当然突破されやすくなることから、新幹線鉄道特例法では列車の運行の安全を確保するための設備をみだりに操作した者を処罰する規定があることも参考になるのではないだろうか。

また、コネクテッドカーの普及とともに、自動車保有者自身の改造により、信号機などインフラに対して自己に都合の良い信号を発することによって混乱を生じさせる行為も懸念されている。

他には、コネクテッドカーの普及とともに、自動車保有者自身の改造により、信号機などインフラに対して自己に都合の良い信号を発することによって混乱を生じさせる行為が懸念され、このような行為には道路交通法第 115 条を適用し得るところであるが、今後の技術革新へ対応するため、更なる法整備の必要性について不断の検討を行っていく必要があるだろう。

（3）不正アクセス禁止法

不正アクセス禁止法は、限定列挙方式になっているが、ライフスタイル認証などの新しい認証にどう対応していくかを検討する余地があるのではないだろうか。

（4）通貨偽造罪（デジタル通貨）

世界的にデジタル通貨の使用や実証実験が加速している。デジタル通貨が発行される場合には、見直しが必要になるだろう。

7．今後の各業法の規制改革への応用

規制改革は、「事前規制から事後規制へ」の方向で進めることが技術革新へ対応するためにも有益である。このためには、事前規制の緩和と事後規制による不正な方法の抑止の双方がセットでなされる改革を追求することも規制改革の一つの類型的な手法として念頭に置くことができるのではないか。

（以上）