サイバー犯罪の研究（五）-サイバーテロ及びサイバー戦に関する比較法的検討-

法律論叢　第八六巻　第二・三合併号（二〇一三・一〇）

【論　説】

サイバー犯罪の研究（五）

――サイバーテロ及びサイバー戦に関する比較法的検討――

夏　井　高　人

目　次

一　はじめに

「サイバーテロ（Cyber terrorism）」及び「サイバー戦（Cyber war）」に関して、国際的に承認された公式の定義は、現在のところ存在しない。

これらの用語は、論者や文脈等によって異なる意義・機能を有するものとして用いられることが多々あり、また、ジャーナリズムの領域で用いられる場合にはしばしば誇張的に用いられている。

しかし、それがいずれの国であるにせよ、特定の国家または特定の国家の統制下にあるサイバー軍（Cyber army）による他国の情報システムに対するサイバー攻撃（Cyber attack）は現実に存在するものと考えられている。(1) そして、

このような国家によって実行されるサイバー攻撃（State sponsored Cyber attack）のことをサイバーテロまたはサイバー戦と呼ぶ例が比較的多いように思われる。[2] 無論、理論的には、単なる個人または国家とは別の社会的組織（国際的なテロ組織など）によって重大なサイバー攻撃が実行されることがあり得るし、それによって生ずる被害は国家等によるサイバー攻撃と同等またはそれ以上のものであり得る。例えば、物理的なテロ攻撃ではあるが、二〇〇一年九月一一日にアメリカ合衆国で発生した同時多発テロ攻撃は、アメリカ合衆国の公式見解によれば過激な国際テロ組織とみなされたアルカイダによるものとされており、特定の国家によるものではない。[3] しかし、一般に、国家によるサイバー攻撃では、その攻撃の規模、持続性（執拗性）、被害の程度及び問題解決の困難性において、個人や国際的なテロ組織等によるサイバー攻撃の場合を上回るものだということは否定できないように思われる。[4]

他方、サイバーテロまたはサイバー戦（以下、本論文では「サイバーテロ」と総称する。）は、物理的な攻撃を主体とする通常のテロとは異なる要素を有している。それは、電子的な攻撃を主体とするものであり、爆撃やミサイルといった目に見える物理的な攻撃手段を主体とするものではないが、攻撃によって生ずる経済的・政治的損失は核攻撃に匹敵するかまたはそれ以上のものとなり得るものだということである。[5] 例えば、Stuxnet のような巧妙なマルウェアによって原子力発電所や化学プラントなどを制御不能状態または混乱状態に陥れるサイバー攻撃が実行され、それが成功した場合、原子力発電所やプラントの爆発を誘発させることが可能であり、その結果、核攻撃や毒ガス兵器による攻撃がなされたのと同じ悲惨な結果が生ずる危険性がある。[6] また、単に発電施設や送電網、ガスパイプライン、上下水道等の管理システムを機能不全にするだけで、高度に電子化されてしまっている都市や国家の機能を麻痺させ、経済活動を不可能にしてしまうことができる。[7]

そうであるにもかかわらず、攻撃それ自体は、ごく平穏な社会生活が営まれている間に電子的に実行されることに

なるから、一般市民の感覚からすれば、平時の状態しか存在していないように見えてしまう。換言すると、サイバーテロが実行可能な環境では、理論的には、戦時と平時とが（明確な社会的・政治的な切り替えが意識されないまま）常に共存する状況にあるということができる。このことは、物理的な戦争状態にある場合とサイバーテロの場合との顕著な相違点の一つとして考えることができる。(8)

無論、政府のインターネットサイト等に対する攻撃が実行され、現実に利用不能状態が発生していれば、当該国の一般国民の目にも「サイバー戦」が存在することが明らかになる。(9)にもかかわらず、インターネットを含め各種情報システムと無関係のところでは全くもって平穏な平時の状態が同時に存在していることが普通となっている。

日本国は、以上のような意味でのサイバーテロと全く無関係でいることはできない。(10)日本国が他国に対してサイバー攻撃を実行する意図を全く有していないとしても、他国から日本国に対してサイバー攻撃が実行されることは十分にあり得る。それゆえ、そのような場合における法的対応（特に犯罪としての刑事処罰）について検討しておく意味がある。国家それ自体を処罰対象とすることは、国家主権の範囲外のことなので、無論できないことだが、サイバーテロを構成する個々の実行行為について、その実行行為者に対する刑法その他の刑罰法令による処罰は全く不可能なことではないからである。

本論文では、サイバーテロの全てについて論ずることはできない。しかし、これまで世界的に注目されてきたサイバーテロのカテゴリの中で、①国家による諜報活動及び②国家の重要施設等に対する侵害に特に着目し、これらの事項に関し重点的に検討を加えることは可能な範囲内にあると思われる。

本論文は、これらの重点的な事項について、アメリカ合衆国連邦刑法(11)及びスイス刑法典（二〇一三年七月一日現在有効な条項）(12)に含まれる関連条項と比較しながら、(13)日本国の刑罰法令（主として刑法に定める関連条項等）によるサ

イバーテロ行為処罰の可否を検討し、それによって今後のこの分野における法学研究に資することを目的とする。

二　国家による諜報活動

1　類型

今日、国家による他国に対する諜報活動は、多方面にわたっており、伝統的な軍事機密情報に対する諜報活動だけではなく、先進国の最先端技術を不法に無償で入手し自国の技術水準や国際経済上の競争力を向上・強化するためになされる産業・技術情報に対する諜報活動の存在も指摘されている(14)。これは、第二次世界大戦以降、戦争というものが職業軍人や徴兵された兵士等のみが関与するものではなく国民全てを巻き込んだ総力戦であることが常態化したという歴史的経緯に鑑みると、ある意味で必然的な結果だと考えることができる。

諜報活動は、工作員による物理的な工作活動の場合もあるし、電子的にリモートで実行されることもある。電子的に実行される諜報活動は、「サイバースパイ（Cyber spy or Cyber espionage）」と呼ばれることもある。また、このような電子的な諜報活動のうち、産業・技術情報に対する諜報活動は、「国家による産業・技術のスパイ行為（state-sponsored industrial and technical espionage）」と表現されることがある(15)。

これら電子的な諜報活動は、実際には、通信傍受(16)や不正アクセスの実行により実現されるが、そのための準備的・手段的な行為として、DDoS 攻撃(17)、APT 攻撃やフィッシング攻撃(18)などが実行されることがしばしばある。これらの行為については、それぞれ適用可能な処罰法令（刑法、不正アクセス禁止法等）による処罰の可否が検討されなければ

ならないが、それらとは別に、外国等による日本国の重要な機密情報をターゲットとする諜報活動それ自体について何らかの処罰立法を要するか否かが検討課題となる。無論、その結論については賛否両論があり得る。(19) しかし、まず結論ありきではなく、世界各国の法制の状況及びその立法の基礎となっている政治的・社会的・経済的・歴史的背景を正確に理解することが重要であると考える。仮にこの種の立法に反対する立場を採る場合であっても、世界各国の立法という事実に関する正確な認識・理解を抜きにして、単純に「反対のための反対」を繰り返すだけでは全く無力だと言わざるを得ない。

以下、ここでは、軍事機密情報と経済機密情報とに分け、軍事機密情報に関してはスイス刑法上の主要な関連条項に、経済機密情報に関してはスイス刑法及びアメリカ合衆国連邦刑法にそれぞれ着目して比較法的な検討を試みる。(20)

2　軍事機密情報に対する諜報活動

(1)　日本法

日本国の刑法上、国家機密に対する侵害罪は存在しない。軍事機密情報と関連する刑法上の犯罪としては、外患誘致罪（八一条）及び外患援助罪（八二条）があるが、これらの条項の解釈としては、外国から物理的に「武力の行使」があった場合にのみ犯罪が成立すると解するしかなく、武力の行使を伴わない純然たる諜報活動についてこれらの条項が適用される余地はないものと思われる。(21)

しかしながら、自衛隊法、日米相互防衛援助協定等に伴う秘密保護法、外国為替及び外国貿易法等の特別法中には軍事機密と関連する条項を有するものがある。

自衛隊法（昭和二九年法律第一六五号）五九条一項は「隊員は、職務上知ることのできた秘密を漏らしてはならない。その職を離れた後も、同様とする」と定め、これに違反して秘密を漏らした者は一年以下の懲役または三万円以下の罰金に処せられる（同法一一八条一項一号）。処罰対象は、自衛隊員のみであるので、サイバーテロとしての諜報活動を行う者（自衛隊員でない者）については、直接に同法五九条一項の違反に該当することはないが、理論的には、教唆犯としての刑事責任を負うことがあり得る。本来、諜報活動を行っている者が犯罪学上では（教唆犯ではなく）主犯として評価されるべきであろうが、現行の自衛隊法上では処罰対象が自衛隊員のみとなっていることから、そのような法解釈となる。

また、日米相互防衛援助協定等に伴う秘密保護法（昭和二九年法律第一六六号）は、次のように定めている。この法律は、日本国の法令中で最も厳格に軍事機密情報を保護するものであると考えられる。(22)

第一条（定義）

1　この法律において「日米相互防衛援助協定等」とは、日本国とアメリカ合衆国との間の相互防衛援助協定、日本国とアメリカ合衆国との間の船舶貸借協定及び日本国に対する合衆国艦艇の貸与に関する協定をいう。

2　この法律において「装備品等」とは、船舶、航空機、武器、弾薬その他の装備品及び資材をいう。

3　この法律において「特別防衛秘密」とは、左に掲げる事項及びこれらの事項に係る文書、図画又は物件で、公になっていないものをいう。

一　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された装備品等について左に掲げる事項

イ　構造又は性能

ロ　製作、保管又は修理に関する技術
ハ　使用の方法
ニ　品目及び数量

二　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された情報で、装備品等に関する前号イからハまでに掲げる事項に関するもの

第二条（特別防衛秘密保護上の措置）

特別防衛秘密を取り扱う国の行政機関の長は、政令で定めるところにより、特別防衛秘密について、標記を附し、関係者に通知する等特別防衛秘密の保護上必要な措置を講ずるものとする。

第三条（罰則）

1　左の各号の一に該当する者は、一〇年以下の懲役に処する。

一　わが国の安全を害すべき用途に供する目的をもつて、又は不当な方法で、特別防衛秘密を探知し、又は収集した者

二　わが国の安全を害する目的をもつて、特別防衛秘密を他人に漏らした者

三　特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を他人に漏らしたもの

2　前項第二号又は第三号に該当する者を除き、特別防衛秘密を他人に漏らした者は、五年以下の懲役に処する。

3　前二項の未遂罪は、罰する。

第四条

1　特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らしたものは、二年以下の禁こ又は五万円以下の罰金に処する。

2　前項に掲げる者を除き、業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らした者は、一年以下の禁こ又は三万円以下の罰金に処する。

第五条

1　第三条第一項の罪の陰謀をした者は、五年以下の懲役に処する。

2　第三条第二項の罪の陰謀をした者は、三年以下の懲役に処する。

3　第三条第一項の罪を犯すことを教唆し、又はせん動した者は、第一項と同様とし、同条第二項の罪を犯すことを教唆し、又はせん動した者は、前項と同様とする。

4　前項の規定は、教唆された者が教唆に係る犯罪を実行した場合において、刑法（明治四〇年法律第四五号）総則に定める教唆の規定の適用を排除するものではない。

加えて、外国為替及び外国貿易法（昭和二四年法律第二二八号）は、特定技術に関する情報及び特定技術である物品の情報通信及び輸出等について規定しており、その罰則が適用される場合がある。同法二五条一項、二項、三項及び六九条の六第二項、三項は次のように規定している。

第二五条　役務取引等

1　国際的な平和及び安全の維持を妨げることとなると認められるものとして政令で定める特定の種類の貨物の設計、製造若しくは使用に係る技術（以下「特定技術」という。）を特定の外国（以下「特定国」という。）において提供することを目的とする取引を行おうとする居住者若しくは非居住者又は特定技術を特定国の非居住者に提供することを目的とする取引を行おうとする居住者は、政令で定めるところにより、当該取引について、経済産業大臣の許可を受けなければならない。

2　経済産業大臣は、前項の規定の確実な実施を図るため必要があると認めるときは、特定技術を特定国以外の外国において提供することを目的とする取引を行おうとする居住者若しくは非居住者又は特定技術を特定国以外の外国の非居住者に提供することを目的とする取引を行おうとする居住者に対し、政令で定めるところにより、当該取引について、許可を受ける義務を課することができる。

3　経済産業大臣は、次の各号に掲げる場合には、当該各号に定める行為をしようとする者に対し、政令で定めるところにより、当該行為について、許可を受ける義務を課することができる。

一　第一項の規定の確実な実施を図るため必要があると認めるとき　同項の取引に関する次に掲げる行為

イ　特定国を仕向地とする特定技術を内容とする情報が記載され、又は記録された文書、図画又は記録媒体（以下「特定記録媒体等」という。）の輸出

ロ　特定国において受信されることを目的として行う電気通信（電気通信事業法（昭和五九年法律第八六号）第二条第一号に規定する電気通信をいう。以下同じ。）による特定技術を内容とする情報の送信（本邦内にある電気通信設備（同条第二号に規定する電気通信設備をいう。）からの送信に限る。以下同じ。）

二　前項の規定の確実な実施を図るため必要があると認めるとき　同項の取引に関する次に掲げる行為

イ　特定国以外の外国を仕向地とする特定記録媒体等の輸出

ロ　特定国以外の外国において受信されることを目的として行う電気通信による特定技術を内容とする情報の送信

第六九条の六　罰則

2　次の各号のいずれかに該当する者は、一〇年以下の懲役若しくは一〇〇〇万円以下の罰金に処し、又はこれを併科する。ただし、当該違反行為の目的物の価格の五倍が一〇〇〇万円を超えるときは、罰金は、当該価格の五倍以下とする。

一　特定技術であって、核兵器、軍用の化学製剤若しくは細菌製剤若しくはこれらの散布のための装置若しくはこれらを運搬することができるロケット若しくは無人航空機のうち政令で定めるもの（以下この項において「核兵器等」という。）の設計、製造若しくは使用に係る技術又は核兵器等の開発、製造、使用若しくは貯蔵（次号において「開発等」という。）のために用いられるおそれが特に大きいと認められる貨物の設計、製造若しくは使用に係る技術として政令で定める技術について、第二五条第一項の規定による許可を受けないで同項の規定に基づく命令の規定で定める取引をした者

二　第四八条第一項の特定の種類の貨物であって、核兵器等又はその開発等のために用いられるおそれが特に大きいと認められる貨物として政令で定める貨物について、第二五条第四項の規定による許可を受けないで同項の規定に基づく命令の規定で定める取引をした者又は第四八条第一項の規定による許可を受けないで同項の規定に基づく命令の規定で定める輸出をした者

3　第一項第二号及び前項第二号（貨物の輸出に係る部分に限る。）の未遂罪は、罰する。

(2)　スイス法

政府情報及び軍事情報を含め国家機密情報に対する侵害行為について、スイス刑法は次のように定めている。

第二七二条　政治的な機密情報

1．外国、外国の政党もしくは組織の利益のために、スイス、その国民、住民もしくは組織にとって不利益となるように、政治的な機密情報を収集した者、その役務を提供した者またはその役務を提供するために他の者の組織を扇動もしくは教唆した者は、三年以下の拘禁刑または罰金刑に処す。

2．重大な場合には、刑罰は一年以上の拘禁刑とする。重大な場合とは、とりわけ、行為者が、連邦の国内的な安全もしくは対外的な安全を損なうような行為を教唆する場合またはそのような虚偽の文書を作成する場合である。

［原文］

Art. 272 Politischer Nachrichtendienst

1. Wer im Interesse eines fremden Staates oder einer ausländischen Partei oder einer andern Organisation des Auslandes zum Nachteil der Schweiz oder ihrer Angehörigen, Einwohner oder Organisationen politischen Nachrichtendienst betreibt oder einen solchen Dienst einrichtet,

wer für solche Dienste anwirbt oder ihnen Vorschub leistet,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

2. In schweren Fällen ist die Strafe Freiheitsstrafe nicht unter einem Jahr. Als schwerer Fall gilt es insbesondere, wenn der Täter zu Handlungen aufreizt oder falsche Berichte erstattet, die geeignet sind, die innere oder äussere Sicherheit der Eidgenossenschaft zu gefährden.

第二七四条　軍事上の機密情報

1. 外国のために、スイスにとって不利益となるように、軍の機密情報を収集した者、その役務を提供した者またはその役務を提供するために他の者の組織を扇動もしくは教唆した者は、三年以下の拘禁刑または罰金刑に処す。

重大な場合には、刑罰は一年以上の拘禁刑とする。

2. 通信文及びその用具は没収する。

［原文］

Art. 274 Militärischer Nachrichtendienst

1. Wer für einen fremden Staat zum Nachteile der Schweiz militärischen Nachrichtendienst betreibt oder einen solchen Dienst einrichtet, wer für solche Dienste anwirbt oder ihnen Vorschub leistet,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

In schweren Fällen kann auf Freiheitsstrafe nicht unter einem Jahr erkannt werden.

2. Die Korrespondenz und das Material werden eingezogen.

これらの条項に定める機密情報の収集の方法には限定がないので、電子的な方法による機密情報の収集の場合も含

まれると解される。また、電子的な通信文は同法二七四条二項の没収の対象となるものと解される。

3　経済機密情報に対する諜報活動

(1)　日本法

経済的な機密情報が特許法に規定する特許権や不正競争防止法に定める営業秘密に該当する場合、それらに属する情報を違法に収集する行為が特許法違反行為または不正競争防止法違反行為として処罰対象となり得ることは言うまでもない(23)。

このような行為が外国に対する協力者等によって日本国内で実行された場合において、犯罪学上では主犯となるべき外国等は単に教唆犯としての立場にたち、実際に実行行為を行った者のみがこれらの法令の違反行為者として処罰されることになると解される。このことは、既述の軍事上の機密情報に対する諜報活動に協力した自衛官と外国等との関係に類似している。

また、特許法上の特許権にも不正競争防止法上の営業秘密にも属しない情報であっても、その機密性を有する産業情報が著作物として著作権法によって保護される場合、少なくとも理論上では、著作権法違反の罪（複製権侵害等の罪）が成立し得ると解される。

以上のように、経済的な機密情報は、基本的に、私人の財産権の一部である知的財産権の一種として法的に保護されている。

しかし、これら個別の法令違反となるか否かが明確ではない機密情報の収集行為を外国等が実行した場合、そのよ

うな行為を一般的に処罰するための法令は存在しない。近時の法改正により罰則が強化された不正競争防止法の罰則においても、同様である。(24)

(2) スイス法

経済的機密情報に対する侵害行為について、スイス刑法は、刑法一六二条において日本国と同様に私人の知的財産権の一種としての刑法的保護を与えている一方で、他方では、刑法二七三条において国防または国家産業全体の保護という観点から経済的機密情報に対する侵害行為を処罰するものとしている。

第二七三条　産業上の機密情報

外国の官庁、外国の組織もしくは私企業またはそれらの代理人のために、生産上の機密もしくは営業秘密を取得した者、または、外国の官庁、外国の組織もしくは私企業またはそれらの代理人のために、生産上の機密もしくは営業秘密を利用可能にした者は、三年以下の拘禁刑または罰金刑に処し、重大な場合には、刑罰は一年以上の拘禁刑とする。拘禁刑に罰金刑を併科することができる。

［原文］

Art. 273 Wirtschaftlicher Nachrichtendienst

Wer ein Fabrikations- oder Geschäftsgeheimnis auskundschaftet, um es einer fremden amtlichen Stelle oder einer ausländischen Organisation oder privaten Unternehmung oder ihren Agenten zugänglich zu machen,

wer ein Fabrikations- oder Geschäftsgeheimnis einer fremden amtlichen Stelle oder einer ausländischen Organisation oder privaten Unternehmung oder ihren Agenten zugänglich macht,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe, in schweren Fällen mit Freiheitsstrafe nicht unter einem Jahr bestraft. Mit der Freiheitsstrafe kann Geldstrafe verbunden werden.

スイス刑法一六二条は、同法二七三条とは別に、生産上の機密もしくは営業秘密に対する侵害の罪を定めている。(25) 同法一六二条の法定刑は三年以下の拘禁刑または罰金刑と規定されており、両者で同一の法定刑となっている。ただし、同法一六二条では拘禁刑と罰金刑との併科条項がなく、重大な場合の加重条項もない。加えて、同法一六二条の行為主体は、法令または契約により生産上の機密もしくは営業秘密を守るべき義務を負っている者のみに適用される（身分犯）。これに対し、同法二七三条は、そのような義務のない者であっても外国等の利益のためにする目的を有する者に対しては適用される（目的犯）。両者の条項においては、これらの点が異なっている。

第一六二条　生産上の機密もしくは営業秘密の侵害

法令または契約に基づき生産上の機密もしくは営業秘密を開示しない義務を負っている者が、自己または第三者の利益のために、その義務に背く行為を実行したときは、三年以下の拘禁刑または罰金刑に処す。

［原文］

Art. 162 Verletzung des Fabrikations- oder Geschäftsgeheimnisses

Wer ein Fabrikations- oder Geschäftsgeheimnis, das er infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte, verrät,

wer den Verrat für sich oder einen andern ausnützt,

wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

(3) アメリカ合衆国法

アメリカ合衆国の連邦刑法（合衆国連邦法律集一八款九〇章）には、スイス刑法や日本国の不正競争防止法等と同様の内容の経済的機密情報の保護のための条項が存在する。ただし、その法定刑は非常に厳しいものであり、世界的にも最も強い厳罰主義を採用した立法例だと考えられている。そして、アメリカ合衆国の処罰条項は、サイバーテロとしての産業上の機密情報をターゲットとする外国等による諜報活動に対しても適用される。

アメリカ合衆国の連邦刑法では、一八三一条においてとりわけ外国等の利益のために実行される営業秘密（Trade secret）のスパイ行為（Espionage）に対する処罰を、一八三二条において営業秘密の侵害に対する処罰一般について定めている。論理的には、一八三二条が営業秘密の侵害を処罰する場合の基本条項であり、一八三一条は外国等を利する目的を有する場合に目的犯として加重処罰する趣旨の条項だと理解することができる。(26)

第一八三一条　産業スパイ

(a)　一般―外国政府、外国の政府代行機関、外国の政府機関を利する侵害行為となることを意図しもしくは認識しながら、認識して、(27)次のいずれかの行為を実行した者は、(b)項の場合を除き、五〇万ドル以下の罰金刑もしくは一五年以下の拘禁刑に処し、またはこれらを併科する。

(1)　営業秘密(28)を盗み、無権限で着服し、奪い、持ち去り、もしくは、詐欺、詐術もしくは欺瞞行為により入手すること；

(2) 営業秘密を、無権限で複写し、複製し、素描し、描画し、撮影し、ダウンロードし、アップロードし、改変し、破壊し、写真複製し、複製物を製造し、移転し、配布し、送信し、電子メールし、通信しもしくは輸送すること；

(3) それが無権限で盗まれ、着服され、入手されもしくは変換されたものであることを認識して、営業秘密を受領し、購入しもしくは所持すること；

(4) (1)ないし(3)に規定する行為中のいずれかを実行しようと試みること；または、

(5) 一名以上の他の者と(1)ないし(3)に規定する行為中のいずれかの実行を共同謀議し、かつ、そのような一名以上の共同謀議者が当該共同謀議の目的を実現する何らかの行為を実行する場合。

(b) 組織[29]—(a)項に規定する違反行為を実行する組織は、一〇〇〇万ドル以下の罰金刑に処する。

［原文］

Sec. 1831. Economic espionage

(a) In General.–Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly–

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

(b) Organizations.–Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

第一三八二条　営業秘密の盗取

(a)　州際取引もしくは国際取引のために製造されまたはこれらの取引において製造された製品と関連する営業秘密またはそのような製品に含まれる営業秘密を移転する意図で、[30]当該営業秘密の保有者以外の者の経済的利益のために、かつ、当該違反行為が当該営業秘密の保有者を害するであろうことを意図しもしくは認識しながら、認識して、[31]次のいずれかの行為を実行した者は、(b)項の場合を除き、本款に規定する罰金刑もしくは一〇年以下の拘禁刑に処し、またはこれらを併科する。

(1)　そのような情報を盗み、無権限で着服し、奪い、持ち去り、もしくは、詐欺、詐術もしくは欺瞞行為により入手すること；

(2)　そのような情報を、無権限で複写し、複製し、素描し、描画し、撮影し、ダウンロードし、アップロードし、改変し、破壊し、写真複製し、複製物を製造し、移転し、配布し、送信し、電子メールし、通信しもしくは輸送す

ること；

(3) それが無権限で盗まれ、着服され、入手されもしくは移転されたものであることを認識して、そのような情報を受領し、購入しもしくは所持すること；(32)

(4) (1)ないし(3)に規定する行為中のいずれかを実行しようと試みること；または、

(5) 一名以上の他の者と(1)ないし(3)に規定する行為中のいずれかの実行を共同謀議し、かつ、そのような一名以上の共同謀議者が当該共同謀議の目的を実現する何らかの行為を実行する場合。

(b) 組織―(a)項に規定する違反行為を実行する組織は、五〇〇万ドル以下の罰金刑に処する。

［原文］

Sec. 1832. Theft of trade secrets

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly–

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

4　知的財産権に属しない経済的機密情報

特許権や営業秘密などの知的財産権の一部として理解することが可能な情報財の侵害を構成するとは認められない情報財であって機密性を有する情報財についても経済的機密情報の保護に関する各国の刑罰法令が適用可能であるかどうかについては、必ずしも明確ではない。

そのような知的財産権としての法的保護を受けない情報財であって機密性を有するものに含まれるものとして、今後、社会的・経済的重要性を増すと予想されるものの中には、例えば、三次元プリンタ（3D Printer）で製造される機器類の設計図に相当する印刷データ等も含まれる。このような印刷データは、現在では設計図面と同じようなものだと理解されている。しかし、通常の設計図の場合、職人等による加工を経て製品が形成・製造されるのに対し、三次元プリンタによって世界中のどのような場所においても即時に完全な製品を全く人の手を経ないで自動的に製造可能であるという点が根本的に異なっている。そのような三次元プリンタ用の印刷データさえあれば、完成された製品を

観察・解析してリバースエンジニアリングすることを要せず、また、設計図から現実の製品等を製造するための特殊な工具、技術、ノウハウといったものを必要としない。換言すると、三次元プリンタを用いた製品等の製造においては、設計図に相当する印刷データから物理的な製品等へと製造・加工する際に生ずる誤差等といったものが原理的に存在しないことになる。

そのような三次元プリンタの利用が急速に発展しており、非常に微細な精密機械から宇宙ロケットのエンジン部品[33]のような非常に大きなものまで様々なサイズのものへの三次元プリンタの応用が始まっている。三次元プリンタは、X線や超音波などでスキャンして得られたデータに基づき本人の骨格を精密に複製して製造された人工骨格を移植するといった医学・医療分野での利用、各種機器類の部品の製造のための利用、玩具などの娯楽用品の製造のための利用のほか、銃砲[34]その他の兵器の部品製造等のような軍事用に用いられることもある[35]。

しかし、この問題については、罪刑法定主義の観点から、消極に解するのが妥当と思われる。

諸外国の関連立法例の解釈としても、全ての種類の経済的機密情報をくまなく情報財として対外的に保護するのではなく、知的財産権として重要なものについて対外的にも保護するという立法政策を採用しているものと思われる。

現実問題として、全ての種類の経済的機密情報の流通を完全にブロックした場合、逆に経済活動の円滑な運営を損なう結果となることが予想され、また、各国との経済取引や貿易にも支障が生ずるおそれがあることから、どの程度の法的・経済的・政治的な重要性をもった経済的情報を情報財として刑事法によって保護すべきかについては慎重な配慮が要求される。

そして、保護対象となるべき情報財としての経済機密情報に対して直接の法的保護を与えるのでなくても、他の法令を適用し処罰することが一般に可能と思われる。例えば、三次元プリンタで用いられる機器類やデータに対する無

権限アクセスや通信傍受といった手段的行為に対する処罰を検討するほうが合理的だと考えられる。また、無権限で入手される機密データが著作物に該当する場合には著作権法に定める罰則の適用も考慮可能である。

ただし、諸外国の立法例はともかくとして、日本国においては、データ（電磁的記録）に対する無権限アクセスの保護法制が極めて貧弱だという点には留意しなければならない。今後の重要な検討課題の一つだと言えよう。

三　国家の重要施設等に対する攻撃

1　攻撃の態様

サイバーテロとしての攻撃の態様は、直接的な物理攻撃と電気通信回線等を介した間接的な物理攻撃の概ね二種類に分けて考えることができる。

直接的な物理攻撃には、①コンピュータウイルス、ロジックボンブその他のマルウェアを用いて各種制御システムを混乱させたり破壊したりするようなタイプの攻撃類型（爆破型）と、②電磁波砲、ビーム砲、レーザー光線砲等の銃砲類似電子的兵器を用いて対象施設を破壊したり、管理要員を発狂・混乱させたり殺傷したりするようなタイプの攻撃（砲撃型）を考えることができる。

②の砲撃型の攻撃の場合、通常の銃砲と同様の扱いにより地上の比較的至近距離から発射されるものと、宇宙空間を周遊する軍事攻撃用人工衛星または軍事用宇宙基地、月面上の軍事基地等から発射されるものとを考えることができる（いわゆるハッキングにより軍事用宇宙施設等の制御を奪い、軍事用の電子兵器を無権限で作動させるような場

合を含む。）。ただし、②の砲撃形の攻撃中の後者については、宇宙法及び空法の分野に関連する事項を含むものであり、専門外の事項を多々含むものであるので、本論文では詳論しない。

直接的な攻撃のターゲットは、物的施設であることも人間であることもある。最も単純な例としては、電磁波防御力の弱い心臓ペースメーカを移植手術により体内に埋め込んでいる者に対して強力な電磁波を照射して当該心臓ペースメーカをショートさせ機能停止させることができる場合には、電磁波の照射という攻撃手段による殺人が可能である。[36] このほか、一般の家電製品等の中には電磁波攻撃に対する防御が脆弱であるものが決して少なくない。[37] また、強力なレーザー光線を照射して失明させたり火傷を負わせたりすることも十分に可能である。[38] そして、脳機能を障害・操作する機能を有する武器が用いられた場合、死亡、発狂、脳損傷、疾病の発病等の結果が生ずることがあり得る。それだけではなく、脳機能をターゲットとする高度な電磁波兵器の中には（少なくとも理論的には）人間の思考をハイジャックし遠隔操作することによって、他人を自分の道具としてマリオネットのように操作するような攻撃を想定することは可能である。そして、その操作される人間が、例えば、原子力発電所の管理要員である場合、当該管理する原子力発電所の原子炉を暴走・暴発させることが可能となる。この場合の操作されている管理要員は、他人によって思考を支配されているのであるから、間接正犯の道具に該当すると考えることができる。また、そこまでいかないにしても、例えば、電子的な視聴覚機能補助装置を装着している者に対し、特定の電磁波攻撃を実行することにより、幻覚や幻聴に類似する状態を発生させることは、現時点でも既に完全に可能である。[39] そして、近未来的には、電子工学の応用に加え生体の遺伝子工学等を応用した他人の思考のハイジャッキングと遠隔操作がかなり現実味を帯びた出来事として発生し得ると考えられる。[40]

しかしながら、これらの攻撃が現実に実行されることを想定した法的検討が公式になされたことはないものと思わ

れる。

特に深刻なのは「グリッド（GRID）」と呼ばれるコンピュータシステム及びネットワークシステムを用いて集中管理するプラント（工場）、電力網[41]、ガスパイプラインなどの制御を破壊したり混乱させたりする攻撃である。しかも、当該ネットワークシステムの管理がインターネットを経由してリモートでなされる場合には、当該ネットワークシステムへの侵入（不正アクセス）によりその制御を奪うことのできる環境が存在していることになる。そして、そのような攻撃が成功すると、現代の社会生活の大半が機能停止となる。

他方、電気通信回線等を介した間接的な物理攻撃は、ほとんど全ての種類の情報ネットワークシステム等について考えることが可能である。

今後、通常の電気通信回線のみならず送電線や水道管等を通信経路とする情報通信が拡大するとすれば、それらを介した攻撃が実行されることは十分にあり得ることであり、また、携帯電話やスマートフォン等の利用を含め無線通信による情報ネットワークの場合には更に深刻な状況の発生を想定すべきである。

加えて、リモートで操作される道路や鉄道などの信号機をハイジャックし遠隔操作すれば、大量殺人が可能となる。同様に、自走式または遠隔操縦式の無人自動車（自動車型ドローン）をハイジャックすれば、まさに文字通り走る凶器としてそれを使用することができることになる[42]。それだけではなく、例えば、国際的なテロリストが爆弾を仕掛けた自動車型ロボットや飛行ロボットなどを遠隔操縦し、重要な施設や官庁ビルなどに突入・爆破させて大規模な物理的破壊テロ攻撃を実行することが可能だと思われる。

コンピュータによって制御される高機能ロボットを凶器として用いる場合、一般論としては、ほとんど全ての種類の犯罪を実行することが可能であり、また、大量のロボットをハック（クラック）してその制御を奪うことに成功す

れば、（少なくとも理論的には）ごく少数の人間だけで武力クーデターを実行し政府を倒すことさえ全く不可能なことではないと言い得る。[43] ロボット（ドローン）は、電子制御によって機能する道具（装置）であるので、ロボットを制御しているコンピュータ・プログラムやそれに対して他のコンピュータシステムや誰かから与えられる命令には（たとえどのような命令であっても）完全に服する。[44] それゆえ、軍事用のロボットの場合、敵軍に制御を奪われたときには自動的に自爆してしまうような仕組みも考えられている。[45] しかし、そのような自爆機能は、同時に、当該ロボットを爆弾兵器として悪用する道をも拓くことになるだろう。

2　電子的手段による物理攻撃

(1)　日本法

直接的な攻撃類型のうち①の攻撃（爆破型）に用いられるマルウェアについては、基本的に、不正指令電磁的記録に関する罪（刑法一六八条の二）を適用して処罰し得ると考える。

しかしながら、直接的な攻撃類型のうち②の攻撃（砲撃型）に用いられる電子的兵器は、金属製の物理弾丸を発射するものではないので、[46]「金属性弾丸を発射する機能を有する装薬銃砲」でも「空気銃」でもないため、現行の銃砲刀剣類所持等取締法（昭和三三年法律第六号）の適用外である。[47] 銃砲刀剣類所持等取締法の抜本改正が急務であると考える。

他方、間接的な物理攻撃の対象が電力、[48] ガス、水道、道路、鉄道、水路その他の重要インフラといった国家の重要施設・設備である場合、刑法上の通常の犯罪が成立し得るので、それによって対処することが可能である。日本国内では比較的少ないけれども、石油採掘プラントや天然ガス採掘プラントなどについても同様に考えることができる。[49]

例えば、不正アクセス行為や不正指令電磁的記録の供用等の手段的行為を通じて各種電子制御システムをハイジャックしたり、混乱・暴走させたり、破壊したり、機能不全にしたりするといった類のサイバーテロによって、化学プラント等で火災を発生させたり、家庭の台所や各種施設の食堂等で炊事用具を異常発熱させて発火させたような場合には放火罪（刑法一〇八条以下）が[50]、軍事施設や[51]発電所、都市ガス貯蔵施設等の爆発物を爆発させた場合には爆発物破裂罪（同法一一七条）が、有害なガスを蓄積している施設からガス漏れを発生させた場合にはガス漏出等の罪（同法一一八条）が、水害の機会に水防施設を機能不全にした場合には水防妨害罪（同法一二一条）が、電子制御により開閉する堤防や水門等[52]を破壊した場合には水利妨害及び出水危険の罪（同法一二三条）が、電子制御されている陸路や[53]水路等[54]の機能を破壊・損壊した場合には往来妨害罪（同法一二四条）が、電子制御されている運行管理システム等の機能を破壊・混乱させた場合には往来危険罪（同法一二五条）が、電車等を転覆させた場合にはその転覆罪（同法一二六条）が、水道の浄水場等を機能不全にした場合には水道汚染罪（同法一四三条）が[55]、水道水の広域配水調整制御[56]を機能不全にした場合には水道損壊罪（同法一四七条）が、工場内の作業用ロボットその他の産業用[57]を暴走させたり、飛行中の航空機[58]を墜落させたり、密閉型施設内の空調システムや防火システム等を混乱させたりすることによって人間を殺傷した場合には傷害罪（同法二〇四条）や殺人罪（同法一九九条）が、ドアの自動ロック機能等を破壊して人間を密室に閉じ込めて外に出ることができないようする場合には監禁罪（同法二二〇条）[59]が、企業の電子決済システムを破壊し企業活動を続行できなくしてしまう場合には電子計算機損壊等業務妨害罪（同法二三四条の二）が、ビル等に設置されている各種作業装置等を暴走させ当該ビルを損傷する場合には建造物損壊罪（同法二六〇条）が、それぞれ適用可能な場合が多いと考えられる[60]。

これらのほか、刑法以外の特別刑法に規定されている各種犯罪についても同様に解することが可能である[61]。

問題は、そのようなサイバーテロの実行可能性が高いかどうかということになるが、利便性を重視する現代社会では、例えば、普通のスマートフォンによって各種機器類を遠隔操作することが可能となってきているところ、一般のスマートフォンその他のモバイル機器では情報セキュリティ上の脆弱性を完全に塞ぐことができないため(62)、サイバーテロの手段としてハイジャックされ利用される危険性は決して無視できるレベルのものではないと考える。

(2) スイス法

スイス刑法においては、ガスや爆発物などによる攻撃がなされる場合には、第七款（二二一条以下）に規定する公共危険罪（Siebenter Titel: Gemeingefährliche Verbrechen und Vergehen）として処罰される。そのための手段は電子的なものであっても法の適用除外はないので、例えば、ガスプラントに対して電磁波砲による攻撃を加えて制御システムを破壊し、プラント全体を暴走・爆発させたり、ビーム砲攻撃によりガスタンクを誘爆させたりする攻撃（直接型の攻撃）だけではなく、インターネット経由でガスプラントを管理するグリッドシステムに侵入してその制御を奪い、ガス爆発を発生させたような場合や、ガスプラントを管理するシステム内にインターネット経由で配達される電子メールに添付ファイル等として仕組んだ攻撃用マルウェアを感染させ、当該システムを混乱させたり破壊したりすることによりガス爆発を発生させたような（間接型の攻撃）には、この款の罪として処罰されることになると解される。

そこで規定されている内容は、日本国の刑法とほぼ同様であるが、日本国の刑法にはない条項も存在する。放射線、電磁波、イオンビームなどを放出させて公共の危険を乗じさせる行為を処罰する条項（二二六条の二）がそうである。

日本国の刑法と比較すると、現代社会において最も危険な存在であり、管理に失敗すると極めて大勢の人々の生命を奪い死滅させかねない危険性を常に内在している原子力施設等に対する攻撃が現実にあり得るということを当然の前提とする処罰条項であるということができる(63)。つまり、スイス刑法においては、原子力発電所等の非常に危険な施

設が破壊され、放射性物質による深刻な汚染が生ずる事態の発生を当然の想定の中に入れていると理解することができる。したがって、例えば、イランの原子力施設に対するStuxnetを用いた攻撃のようなサイバーテロがスイスの原子力発電所等に対して実行され、放射性物質による汚染が生じたときは、この条項が適用されることになる。(64)

第二二六条の二

1　故意に、放射能、放射性物質もしくは放射線を用いて、人もしくは公衆の生命もしくは身体または他人の財産権に深刻な損害を発生させた者は、拘禁刑または罰金刑に処す。拘禁刑の場合には罰金刑を併科する。

2　過失による行為の場合には、五年以下の拘禁刑または罰金刑に処す。拘禁刑の場合には罰金刑を併科する。

［原文］

Art. 226bis Gefährdung durch Kernenergie, Radioaktivität und ionisierende Strahlen

1 Wer vorsätzlich durch Kernenergie, radioaktive Stoffe oder ionisierende Strahlen eine Gefahr für das Leben oder die Gesundheit von Menschen oder fremdes Eigentum von erheblichem Wert verursacht, wird mit Freiheitsstrafe oder mit Geldstrafe bestraft. Mit der Freiheitsstrafe ist eine Geldstrafe zu verbinden.

2 Handelt der Täter fahrlässig, so wird er mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft. Mit der Freiheitsstrafe ist eine Geldstrafe zu verbinden.

また、スイス刑法二三〇条は、施設や装置等の安全装置を違法に解除する行為を処罰対象としている。安全装置を解除するための方法は物理的な手段で直接に実行されることもあるが、例えば、グリッドシステムでは遠隔操作

によって安全装置を操作することが可能であるため、当該システムの制御をリモートで奪い、ネットワーク経由で遠隔地から安全装置を解除するような行為についても同条の規定が適用可能と解される。

第二三〇条

1　工場内もしくはその他の商業施設内または機械装置上に事故防止のために設置された安全装置を、故意に、損傷し、破壊し、除去し、その他利用できなくし、機能しないようにした者、または、法律上の義務に違反して、故意に、そのような安全装置を設置しなかった者は、三年以下の拘禁刑または罰金刑に処す。拘禁刑の場合には罰金刑を併科する。

2　過失による行為の場合には、三年以下の拘禁刑または罰金刑に処す。

［原文］

Art. 230 Beseitigung oder Nichtanbringung von Sicherheitsvorrichtungen

1. Wer vorsätzlich in Fabriken oder in andern Betrieben oder an Maschinen eine zur Verhütung von Unfällen dienende Vorrichtung beschädigt, zerstört, beseitigt oder sonst unbrauchbar macht, oder ausser Tätigkeit setzt, wer vorsätzlich eine solche Vorrichtung vorschriftswidrig nicht anbringt, und dadurch wissentlich Leib und Leben von Mitmenschen gefährdet, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Mit Freiheitsstrafe ist eine Geldstrafe zu verbinden.

2. Handelt der Täter fahrlässig, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

(3)　アメリカ合衆国法

アメリカ合衆国の連邦法中で最も重要なものは、連邦刑法一〇三〇条（USC title 18 1030）である。この条項は、これまで何度か改正され、サイバーテロに対する国防の一部として処罰強化が図られてきた。(65)

このほか、ホームランドセキュリティ（Homeland Security）と関連する各種法令が多数存在するが、その詳細については割愛する。

四　関連する日本の裁判例

公刊されている裁判例は非常に乏しい。そのため、日本国の国民は、本論文のテーマであるサイバーテロ及びサイバー戦と関連するものとしてどのような裁判事例があり、どのような判決がなされたのかについて、網羅的かつ正確に知ることはできない。

ここでは、いずれも非常に有名な事件ばかりであるが、外国為替及び外国貿易法違反行為が問題となった刑事裁判事例を数件例示するのにとどめる。(66)

これらの事案では、いずれも電子的な機密情報の送信などの行為が実行されているわけではなく、機密情報の移転の事例でも物理媒体に記録した状態での移転がなされている。しかし、現在のようなインターネットの時代には情報通信回線を介して電子的に機密情報の移転がなされるのが普通である。物理媒体を用いた機密情報の移転に関する過去の刑事判決における量刑が情報通信回線を介した電子的な移転に事例にそのまま応用可能とは思われないが、一応の判断資料となるのではないかと考える（一部仮名）。

(1)　東芝機械株式会社事件

［主文］

被告人東芝機械株式会社　罰金二〇〇万円
被告人H　懲役一〇月（三年間執行猶予）
被告人T　懲役一年（三年間執行猶予）

［罪となるべき事実］

被告人東芝機械株式会社は、東京都中央区銀座に本店を置き、工作機械等の製造及び販売等を目的とする居住者、被告人Hは同社の工作機械事業部長室室長として工作機械等の製造等に従事していたもの、被告人Tは同社の海外本部工作機械輸出部専任課長として工作機械等の販売等に従事していたものであるが、被告人H及び同Tは、一　Yらと共謀の上、被告会社の業務に関し、同時に制御することができる軸数が九である金属工作機械（数値制御装置の仕組みとしては一つの制御軸を共有する二組の同時五軸制御であり、機械全体としては同時九軸制御となる。）の部分品であるスナウト（カッターヘッド）をソヴィエト社会主義共和国連邦（以下「ソ連」という。）に輸出するには通商産業大臣の書面による承認を受けなければならないにもかかわらず、法定の除外事由がないのに、右承認を受けることなく、昭和五九年六月二〇日ころ、右スナウト一二個（製造原価約二三三六万円相当）を神奈川県横浜市鶴見区所在の横浜港大黒埠頭から船積みしてソ連のイリチエフスク港に向けて輸出し、もって

通商産業大臣の承認を受けないで貨物を輸出し

二　右Y及びSらと共謀の上、被告会社の業務に関し、同時に制御することができる軸数が九である金属工作機械（数値制御装置の仕組みとしては一つの制御軸を共有する二組の同時五軸制御であり、機械全体としては同時九軸制御となる。）の使用に係る技術であるとともに電子計算機の使用に係る技術を、非居住者である全ソ技術機械輸入公団に提供する取引をするには、通商産業大臣の許可を受けなければならないにもかかわらず、法定の除外事由がないのに、右許可を受けることなく、昭和五九年七月一日ころ、前記金属工作機械の部分品であるスナウトを装着して右金属工作機械を作動させるための技術であるとともに電子計算機の使用に係る技術であるパートプログラミングマニュアル、コンピュータ・プログラムズマニュアル、ソースプログラムリスト（制作原価約七三万九〇〇〇円相当）を和光交易株式会社社員Kを介し情を知らない三井物産株式会社社員Iをして手荷物として和光交易株式会社モスクワ支店事務所へ届けさせてソ連に搬出させた上、同月六日ころ、右モスクワ支店事務所において、右Sがこれを全ソ技術機械輸入公団の指定するレニングラードのバルチック工場関係者フィルスコフに交付して提供し、もって通商産業大臣の許可を受けないで役務取引をしたものである。

(2)　株式会社S企業事件（東京地裁平成一六年一〇月一五日判決・平成一五年（特わ）三九四〇号・判例集等未搭載）

［主文］

被告人株式会社S企業　罰金一五〇〇万円

被告人A　懲役二年六月（五年間執行猶予）

被告人Ｂ　懲役一年六月（三年間執行猶予）

［罪となるべき事実］

被告人株式会社Ｓ企業（以下「被告会社」という。）は、東京都渋谷区に本店を置き、粉体工学機器の製造販売、輸出及び輸入等の業務を目的とする会社であり、被告人Ａは、同社の代表取締役としてその業務全般を統括掌理する者であり、被告人Ｂは、同社の海外事業部海外営業課長代理として同社の海外営業業務及び輸出入業務を担当していた者であるが、被告人Ａ及び被告人Ｂは、共謀の上、

第１　株式会社Ｓ企業の業務に関し、平成一一年五月二八日ころ、通商産業大臣の許可を受けることなく、情を知らない通関業者であるＸ株式会社の係員らをして、横浜市中区所在の横浜港において、外国為替及び外国貿易法四八条一項（平成一一年法律第一六〇号による改正前のもの）、輸出貿易管理令一条一項、別表第一の四の(9)（平成一二年政令第三四七号による改正前のもの）、輸出貿易管理令別表第一及び外国為替令別表の規定に基づき貨物又は技術を定める省令三条一〇号（平成一二年通商産業省令第一一五号による改正前のもの）が輸出を規制している推進薬の原料である過塩素酸アンモニウムを粉砕するためのジェットミルである「シングルトラック・ジェットミル―二〇〇」一台（販売価格三七七万二〇〇〇円）を船積みさせて、イラン・イスラム共和国のバンダーアッバス港に向けて輸出し、もって、通商産業大臣の許可を受けないで貨物を輸出し、

第２　被告会社の業務に関し、「シングルトラック・ジェットミル―四七五」一台（販売価格一一五〇万円）の輸出申告を行うに際し、平成一二年一一月一七日ころ、横浜市鶴見区大黒ふ頭一五番地所在の横浜税関大黒埠頭出張所において、同税関大黒埠頭出張所長に対し、情を知らない通関業者であるＸ株式会社の係員らを介して電子

情報処理組織により同貨物の輸出申告を行うに際し、上記電子情報処理組織の電子計算機に備えられたファイルの輸出承認等区分欄に、真実は上記ジェットミルが外国為替及び外国貿易法四八条一項（平成一一年法律第一六〇号による改正前のもの）、輸出貿易管理令一条一項、別表第一の四の(9)、輸出貿易管理令別表第一及び外国為替令別表の規定に基づき貨物又は技術を定める省令三条一〇号が輸出を規制している推進薬の原料である過塩素酸アンモニウムを粉砕することのできるジェットミルであるにもかかわらず、同貨物が通商産業大臣の許可を受ける必要のない貨物として「ＮＯ」と入力して輸出申告を行い、もって、偽った輸出申告をし、

第３　被告会社の業務に関し、平成一二年一一月二二日ころ、通商産業大臣の許可を受けることなく、情を知らない通関業者であるＸ株式会社の係員らをして、前記横浜港において、前記第２のとおり法令により輸出が規制されている前記「シングルトラック・ジェットミル―四七五」一台を船積みさせて、イラン・イスラム共和国のバンダーアッバス港に向けて輸出し、もって、通商産業大臣の許可を受けないで貨物を輸出した。

(3)　**Ｐ株式会社事件（東京地裁平成元年一一月二八日判決・平成元年（特わ）一三九五号・判例集等未搭載）**

［主文］

被告人Ｐ株式会社　罰金五〇〇万円

被告人Ｍ　懲役二年（四年間執行猶予）

［罪となるべき事実］

被告人Ｐ株式会社（以下、被告会社という。）は、東京都千代田区麹町に本店を置き、各種電気・機械器具等の製造・販売等を目的とする会社であり、被告人Ｍ（以下、被告人という。）は、被告会社の代表取締役として、同会社の業務全般を統括していたものであるが、被告人は、

第一　Ｓ、Ｉ及びＴらと共謀の上、被告会社の業務に関し、ハフニウムワイヤーをドイツ民主共和国を仕向地として輸出しようと企て、その旨の税関長の許可を受けず、かつ、法定の除外事由がないのに、通商産業大臣の承認を受けないで、

一　昭和六二年二月二一日、情を知らない株式会社阪急交通社の職員らをして、ハフニウムワイヤー約三キログラム（価格約一三六万二四二〇円相当）を、千葉県成田市三里塚字御料牧場一番地の一所在の新東京国際空港から、航空便でドイツ民主共和国に向けて送り出させ、

二　同年三月八日、情を知らないＫをして、同人が前記空港からドイツ民主共和国に向け旅客機で出国するに際し、ハフニウムワイヤー約七キログラム（価格約三一七万五五七八円相当）を、同人の携帯品として同旅客機に積み込ませてドイツ民主共和国に向けて送り出させ、

もって、税関長の許可を受けず、通商産業大臣の承認を受けないで貨物を輸出し、

第二　Ｇ並びに前記Ｓ、Ｉ及びＴらと共謀の上、被告会社の業務に関し、半導体機器であるマスクアライナー（ＭＰＡ―六〇〇ＦＡ）をドイツ民主共和国に輸出しようと企て、大韓民国に設立した被告会社の関連会社からメーカーであるキャノン株式会社に対し右商品の引き合いを出させ、大韓民国及び中華人民共和国を順次経由してドイツ民主共和国に右商品が到着するようあらかじめ準備工作をした上、その旨の税関長の許可を受けず、かつ、法定の除外事由がないのに、通商産業大臣の承認を受けないで、

一　同六二年六月二七日、情を知らないキャノン株式会社の係員らをして、前記マスクアライナー一セット（価格一億九三七万九九五二円相当）を、前記空港から航空便で大韓民国を経由する方法でドイツ民主共和国に向けて送り出させ、

二　同年八月一日、情を知らない同会社の係員らをして、同マスクアライナー二セット（価格合計一億七三五六万三八九四円相当）を、前記空港から航空便で大韓民国を経由する方法でドイツ民主共和国に向けて送り出させ、

三　同年九月八日、情を知らない同会社の係員らをして、同マスクアライナー一セット（価格一億九二三万四二八六円相当）を、前記空港から航空便で大韓民国を経由する方法でドイツ民主共和国に向けて送り出させ、

もって、税関長の許可を受けず、通商産業大臣の承認を受けないで貨物を輸出したものである。

(4)　日本航空電子工業株式会社事件（東京地裁平成四年四月二三日判決・判例時報一五七二号二七頁）(67)

［主文］

日本航空電子工業　罰金五〇〇万円

被告ら　懲役二年（三年間執行猶予）

［犯罪事実の概要］

1　日本航空電子工業は、昭和五九年三月二八日から昭和六一年九月三〇日までの間、関税法・外為法に違反し、最終仕向地がイランであることを認識しながら、別紙一の一覧表記載のとおり、F―四ジェット戦闘機に使用さ

れる加速度計（F―四戦闘機用慣性航法装置部品リットンA―二〇〇Dアクセロメーター）一一七個、ジャイロスコープ二二八個（同部品リットンG―二〇〇ジャイロスコープ二一三個、F―四戦闘機用火器管制装置部品ハネウエルジャイロスコープGG―一一六三・一五個）（申告価格合計八億六五二七万九三九〇円）を税関長・通産大臣の許可を受けることなく、香港ハイエラックス社及びシンガポールエアロシステムズ社に販売し、引渡した。

2　日本航空電子工業は、昭和六一年一月一〇日から平成元年四月四日までの間、同じく関税法・外為法に違反し、最終仕向地がイランであることを認識しながら、別紙二の一覧表記載のとおり、サイドワインダーミサイル（F―四ジェット戦闘機搭載用空対空ミサイルAM一九型の俗称）の部分品ローレロン三〇七九個（申告価格合計七〇九八万三三七七円、ただし試作品及び返品を含む）を税関長・通産大臣の許可を受けることなく、シンガポールに輸出した。

3　被告らは、昭和六三年五月二二日から平成元年四月四日までの間、ローレロン一三五七個をシンガポールに輸出した。

五　まとめ

以上で本論文における検討を終える。

本論文では、試みにスイス刑法及びアメリカ合衆国連邦刑法との比較というかたちを通してサイバーテロに対抗するための刑事法のありかたについて考察してみた。しかし、もとより、本論文でとりあげた諸外国の立法例がこの分野において特別に優れた内容を有するものであるという趣旨ではないし、また、世界的にみて最も効果的な法制であ

るという理解に基づくものでもない。無論、これら諸外国の立法例には長所も短所もあるし、法解釈や法執行のいかんによっては弊害もあり得る。

他方で、日本国においては、第二次世界大戦前における厳しい情報統制及び思想弾圧という歴史的経験のゆえにスパイ活動等に対する法的対応についてしばしば過敏な反応がみられる。また、日本が置かれている地政学的な特殊条件のために、安易な立法やその提案等が国際的な摩擦や対立を惹起しかねないということも否定することのできない事実である。それゆえ、これらの事項に関する考察・検討には深い思慮と広い国際的視野とが要求されることになる。

しかしながら、「情報財」として理解されている情報の保護という観点からすると、サイバーテロによる情報の無権限取得（諜報活動）やそのような情報の破壊行為について完全に目を瞑ったままでいることもできない。それは、理論的な論理必然性というよりもむしろ政治・経済的な必要という事実からそうなのだと言わざるを得ない。

なお、本論文は、「戦時と平時が常に共存する状況」の下において、平時の法に属する刑法等の通常の刑事法による対処がどこまで可能かという観点からの検討結果の一部である。この非常に難解な法的課題を取り扱う上で最も重要なポイントとなるべき違法性阻却事由の問題については、諸般の事情を考慮し、意図的に検討対象から除外することとした。

本論文がこの分野における法学研究に何らかの寄与となることを期待する。(68)

注

（1） 例えば、近隣諸国の例としては、韓国に対して北朝鮮からサイバー攻撃が実行された事例などがある。

（2） 参考となる文献として、Richard A. Clarke & Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It, Ecco, 2012′ Edward R. Miller-Jones, Cyber Warfare, Fastbook Publishing, 2012′ David B. Farmer, Do the Principles of War Apply to Cyber War?, Biblioscholar, 2012′ Jason Andress & Steve Winterfeld,

Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Syngress, 2011、Josef Schroft, Bahram M. Rajaee & Dieter Muhr (eds.), Hybrid and Cyber War As Consequences of the Asymmetry: A Comprehensive Approach Answering Hybrid Actors and Activities in Cyberspace, Peter Lang, 2011、Mark Sauter & James Carafano, Homeland Security: A Complete Guide 2nd edition, McGraw-Hill, 2011、Jeffrey Carr, Inside Cyber Warfare, Oreilly, 2009、Mark M. Lowenthal（茂田 宏訳）『インテリジェンス―機密から政策へ』（慶應義塾大学出版会、二〇一一）、江畑謙介『情報と戦争』（ＮＴＴ出版、二〇〇六）、喬 良、王 湘穂、坂井臣之助（劉訳）、『超限戦21世紀の「新しい戦争」』（共同通信社、二〇〇一）などがある。

（3）　アメリカ合衆国で発生した同時多発テロ攻撃及びそれによる社会的影響については、岡本篤尚『《9・11》の衝撃とアメリカの「対テロ戦争」法制』（法律文化社、二〇〇九）が参考になる。なお、同時多発テロ攻撃以降におけるアメリカ合衆国連邦政府の対応について批判的な書籍として、David E. Sanger, Confront and Conceal, Crown, 2012 がある。

（4）　それゆえ、本論文では、主として国家等によるサイバー攻撃の場合を想定する立場を採用することにする。

（5）　前掲 Sanger, Confront and Conceal を参照されたい。

（6）　一九八二年、カナダの企業からソヴィエトロシアのスパイが盗み出したシベリアガスパイプライン管理システム用のコンピュータプログラム内にアメリカ合衆国の諜報機関ＣＩＡによって仕組まれていたマルウェア（コンピュータウイルス）によって、ソヴィエトロシアのシベリアガスパイプラインに重大事故が発生したという事例があるとされている。この事例は、ＣＩＡのサイトでも公式に触れられているものの一つである。

Gus W. Weiss, The Farewell Dossier - Duping the Soviets, CIA［二〇一三年七月二三日確認］

ただし、単なる風評の一種に過ぎないという否定的または批判的な見解もある。なお、このような事例に関する関連書籍としては、Thomas Reed, At the Abyss: An Insider's History of the Cold War, Random House LLC, 2007 がある。

（7）　United States Congressional House, Computer Security: Cyber Attacks–War Without Borders: Hearing Before the Subcommittee on Government Management, Information, Books LLC, 2011

（8）　前掲江畑謙介『情報と戦争』一八六頁

（9）　例えば、インド、パキスタン、バングラデシュ、スリランカ等の地域において、宗教上または政治上の対立から、相手国政府の Web サイトに対するサイバー攻撃が実行され、そのような攻撃がなされる度に、攻撃者が攻撃成功の声明を公表し、攻撃を

受けた側の政府が厳しい非難をした上で報復としてのサイバー攻撃をすることになるといった事態が常態化しており、地政学的にみて非常に不安定な状態となっていることは周知のとおりである。

（10） 夏井高人「サイバー犯罪の研究（二）―フィッシング（Phishing）に関する比較法的検討―」法律論叢八五巻四・五合併号一八三頁でも簡単に触れた。

（11） USC title 18 chapter 90 Protection of trade secrets

（12） Schweizerisches Strafgesetzbuch, vom 21. Dezember 1937 (Stand am 1. Juli 2013)

（13） 様々な考慮の上で本論文ではスイス刑法を素材として検討をするのが妥当であると判断した。日本の一般国民にとってスイスは「平和な中立国家」であるとの印象が非常に強い。事実そうであろうと思われるが、そのためにはスイスが国家としての可能な最大の防御を尽くしており、法制もまたその例外ではないという事実を無視することはできない。

（14） the US Office of the Secretary of Defense, Annual Report to Congress - Military and Security Developments Involving the People's Republic of China 2013
http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf［二〇一三年七月二〇日確認］

（15） 前掲 Annual Report to Congress p.45

（16） 夏井高人「サイバー犯罪の研究（三）―通信傍受に関する比較法的検討―」法律論叢八五巻六号三六三頁以下

（17） 夏井高人「サイバー犯罪の研究（一）―DoS 攻撃（DDoS 攻撃）に関する比較法的検討―」法律論叢八五巻一号二〇〇頁以下

（18） 前掲夏井高人「サイバー犯罪の研究（二）―フィッシング（Phishing）に関する比較法的検討―」一八二頁以下

（19） 日本国においては、いわゆるスパイ罪または国家機密漏洩罪の新設を求める法案（主として、公務員や自衛隊員の守秘義務を厳格化・厳罰化することを内容とするもの）が何度も国会で提案されてきたが、いずれも廃案となった。諸外国においては、この種の立法例が多数存在する。しかし、日本国では、とりわけマスコミ等から厳しい批判・反対がある。

（20） この分野における立法例として比較的重要と思われるドイツ刑法及びその法解釈に関しては、Jörg Eisele, Computer- und Medienstrafrecht, C.H. Beck, 2013 が参考になる。

（21） 西田典之『刑法各論第六版』（弘文堂、二〇一二）四一四頁は、「情報の提供」の行為も外患援助行為に含まれ、非戦闘員の行為も含まれるとしている。

（22） 同法制定以降に日本国とアメリカ合衆国との間で締結された国際合意としては、二〇〇七年に締結された「秘密軍事情報の

保護のための秘密保持の措置に関する日本国政府とアメリカ合衆国政府との間の協定（Agreement between the Government of Japan and the Government of the United States of America concerning Security Measures for the Protection of Classified Military Information）」がある。また、二〇一二年、日本国とオーストラリアとの間で「情報の保護に関する日本国政府とオーストラリア政府との間の協定（Agreement between the Government of Japan and the Government of Australia on the Security of Information）」が締結された。

（23）　前掲「サイバー犯罪の研究（三）―通信傍受に関する比較法的検討―」三八五頁

（24）　平成一五年（二〇〇三年）の不正競争防止法一部改正により、不正競争防止法違反の罪として営業秘密の侵害行為が処罰されることとなった。同改正以後の状況については、平成一六年度特許庁産業財産権制度問題調査研究報告書「不正競争防止法を活用した知的財産の保護強化（営業秘密の保護と模倣品・海賊版対策）に関する調査研究報告書」が詳しい。そして、平成二一年（二〇〇九年）の再改正により営業秘密の侵害に対する罰則が強化され、更に、平成二三年（二〇一一年）及び同二四年（二〇一二年）に刑事手続に関する改正がなされて今日に至っている。これらの点については、経済産業省知的財産政策室『逐条解説不正競争防止法―平成二一年改正版』（有斐閣、二〇一〇）及び同『逐条解説不正競争防止法―平成二三・二四年改正版』（有斐閣、二〇一二）を参照されたい。

（25）　スイス刑法一六二条の規定は、実質的には、かつて日本国で昭和四〇年代後半に議論された改正刑法草案三一八条（企業秘密漏示罪）と同じ内容のものである。改正刑法草案三一八条は、「企業の役員又は従業員が、正当な理由がないのに、その企業の生産方法その他の技術に関する秘密を第三者に漏らしたときは、三年以下の懲役又は五十万円以下の罰金に処する。これらの地位にあった者が、その企業の生産方法その他の技術に関する秘密を守るべき法律上の義務に違反して、これを第三者に漏らしたときも同じである」というものであった。

（26）　［訳注］もし日本国の法令中に同種の条項が制定された場合には、加重処罰条項のみが適用される法条競合の関係にたち、観念的競合の関係にはたたないと解される。

（27）　［訳注］ここでの「knowingly」は、基本的に故意犯のみを処罰対象とし過失犯を除外する趣旨と理解される。ただし、構成要件に該当する客観的な事実についての認識のみを要し、構成要件該当行為の実行についての意欲を要件としていない点に留意すべきである。無論、法律の錯誤は故意を阻却しないので、例えば、米国の研究施設等で特定の企業との間で守秘契約が締結された資金提供の下で専門研究に従事していた研究者等が研究に用いたデータを日本国に移転すれば、移転したデータ及び

その移転という客観的事実についての認識さえあれば、故意の要件を充足することになる。この場合、法規制の対象となっているかどうかという点について当該研究者に認識がなかった場合や錯誤ないし誤解がある場合であっても故意を阻却することはない。過失によって場合としては、自己が移転したデータの中に法的保護を受けるデータが含まれているという客観的事実についての認識がなく、そのようなデータが誤って移転したデータの中に混入してしまったような場合などに限定されることになると思われる。

（28）［訳注］「trade secret」を「営業秘密」と訳することにしたが、この条項では営業秘密を記録した物品等のことも含めて規定されている。同法における「営業秘密」の範囲は、日本国の不正競争防止法における「営業秘密」のとは若干異なり、日本法よりもかなり広い。なお、同法における「trade secret」の定義は、同法一八三九条中に規定されている。

（29）［訳注］「組織（organizations）」とは、(a)項で処罰対象となっている自然人ではない法人や団体その他の組織を意味するものと解される。

（30）［訳注］連邦法であるので、州際取引または国際取引と関係のない製品等にかかる営業秘密については本条が適用されない。一八三一条は外国等を利する目的が構成要件要素となっているため自動的に連邦法の所管となるが、一八三二条は通常の商取引と関連する法の立法権分配原則に従い、個々の州内でのみ問題となり得る営業秘密侵害行為については各州の立法権に復することになる。

（31）［訳注］ここでの「knowingly」は、一八三一条におけるのと同様、過失犯を除外する趣旨と解される。

（32）［訳注］「convert」の意義はやや難解であるが、同条及び一八三二条における用語例を整合性のあるものとして合理的に解釈すると、営業秘密に属する情報内容を記録した媒体等から何らかのかたちで複製または保存し、物理的手段、電子的手段その他の何らかの手段を用いて他所（特に外国等）に移転することをその内容とするものと解されるので、「移転」と訳することにした。

（33）例えば、次のような報道がなされている。

Nasa tests 3D-printed rocket engine fuel injector

BBC: 15 July, 2013

http://www.bbc.co.uk/news/technology-23313921［二〇一三年七月二二日確認］

（34）三次元プリンタで製造可能な銃砲の部品データをインターネット経由で配布した場合、それだけでは単に電磁的記録の伝送

に過ぎないが、その部品データを用いて実際に銃砲の部品を製造し組み立てると実射可能な銃砲を完成できることが確認されている。そのようにして製造された銃砲には殺傷能力がある。その実例については多数の報道があるが、例えば、下記のような報道がなされている。

This Is The World's First Entirely 3D-Printed Gun (Photos)
Forbes: May 3, 2013
http://www.forbes.com/sites/andygreenberg/2013/05/03/this-is-the-worlds-first-entirely-3d-printed-gun-photos/
[二〇一三年七月二二日確認]

（35）　軍の部隊を実戦配置し戦闘行為を実行する場合、武器の故障や損耗が必然的に生ずる。そのような場合、補給が途絶えると、当該部隊の戦闘力が大幅に失われる危険性がある。しかし、三次元プリンタを用い部品の印刷データによって必要な部品を必要な数だけ現場（戦場等）で即座に製造して補給することが可能となる。特に機密性を要する部品等については印刷データを部隊が持ち歩くのではなく衛星通信等を介して本国からデータ送信することにより遠隔操作で部隊の三次元プリンタを機能させ必要な部品等を製造することが可能となる。そして、実際に必要となるかどうかわからない部品等を運搬するための輜重部隊の負担を大幅に軽減することが可能となるため、部隊の機動性を大幅に向上させることが可能となる。ロボット兵（ドローン）主体の戦闘部隊のためにはこのような三次元プリンタによる部品製造能力は必須のものとなるだろう。また、人間の兵士主体の戦闘部隊の場合でも、兵士の骨格データ等を予めデータベースに登録しておくことにより、戦場において当該兵士の本物の骨格と同じかたちをした応急手術用人工骨を三次元プリンタで製造しそれを用いて外科手術をすれば、兵士の救命や事後の回復・社会復帰のために役立つだろうと思われる。このように、三次元プリンタは民生品としてのみならず軍用としても極めて重要なものとなってくると考えられることから、仮にそれが民生品として市販されているものであっても軍事機密の一種として扱われることがあり得ることになる。

（36）　厚生労働省医薬品食品局安全対策課長、厚生労働省医薬品食品局審査管理課医療機器審査管理室長「電気自動車の充電器の電磁波による植込み型心臓ペースメーカ等への影響に係る使用上の注意の改訂について（平成二五年三月一九日・薬食安発〇三一九第三号、薬食機発〇三一九第一号）」参照

（37）　電磁波と関連する安全確保の問題に関する一般については、電気学会電磁環境・情報セキュリティ技術調査専門委員会編『電磁波と情報セキュリティ対策技術』（オーム社、二〇一二）が参考になる。

（38）「消費生活用製品安全法（昭和四八年法律第三一号）第三条の規定に基づき、経済産業省関係特定製品の技術上の基準等に関する省令の一部を改正する省令」（平成二四年経済産業省令第八四号）は、高出力のレーザーポインタによる失明などの身体被害があることを前提に、その安全基準を定めている。

（39）仮想現実（Argument Reality）を実現するための各種情報機器類に対する攻撃では、このような攻撃が最も効果的に実行され得るかもしれない。

（40）ここにおいて、フィードバックの機能を有する限り生物と非生物とを架橋する唯一のカテゴリ的概念である「サイバネティクス（Cybernetics）」の真の意義が認識・理解されるに至るであろう。

（41）〝대규모 정전사태、외부 해킹 가능성 있다〟
聯合ニュース：二〇一一年九月一七日
http://www.yonhapnews.co.kr/economy/2011/09/16/0303000000AKR20110916183200017.HTML［二〇一三年七月二四日確認］

（42）故意による自動車型ロボットのハイジャックだけではなく、制御用プログラムのバグ等による異常走行による交通事故、人間ではないコンピュータ制御による走行のゆえに生ずる通常の部品強度の限界を超えた金属疲労等の発生に起因する交通事故、太陽風の影響、地磁気のずれ、人工衛星の故障などによるＧＰＳデータ処理の異常から生ずる交通事故、あるいは、実験室内や閉鎖的な実験用道路ではなく現実の一般道路を走行する場合に生ずる想定外の事態から生ずる交通事故等も想定すべきである。このような場合、当該自動車型ロボットの開発者（当該自動車型ロボット全体の設計者だけではなく、センサーの開発者や制御用プログラムの開発者等を含む。）について、業務上過失致死傷の成立を検討すべきである。同様のことは、航空機型ロボットや船舶型ロボットについても言うことができる。なお、このようなタイプの問題は単なる危惧にとどまるものではなく、既に事故実例が生じている。例えば、「ミリ波レーダーによる障害物検知ソフトが不適切なため、乱反射したミリ波情報を誤って障害物と認識し、衝突の可能性がないのに自動ブレーキが作動する可能性がある」として、トヨタが製造・販売する自動車約二万台をリコールする旨を道路交通省に届け出たという事例がある。ロイターの報道によれば、この問題と関連する不具合の報告が六件、物損事故が一件発生したとされている。
トヨタ、新型「クラウン」など約二万台をリコール
ロイター：二〇一三年六月二六日

http://jp.reuters.com/article/topNews/idJPTYE95P04B20130626［二〇一三年七月二三日確認］

（43）　ロボットは機械装置であるので、人間を殺傷することのできる毒ガスの中でも行動することができる。それゆえ、毒ガスを撒き散らし周囲の人間を皆殺しにしながら攻撃してくるロボット兵の前では、それに抵抗することのできる人間の兵士や警官等が全て毒ガスによって殺傷されてしまい、国家としての国防・治安機能が根底から崩壊してしまうといった最悪の事態が発生し得る。

（44）　ロボットが有する本質的な危険性については、夏井高人『ネットワーク社会の文化と法』（日本評論社、一九九七）六四頁でも触れた。

（45）　DARPA: Your Tech Will Self-Destruct

Information Week: January 30, 2013

http://www.informationweek.com/government/security/darpa-your-tech-will-self-destruct/240147349［二〇一三年七月二三日確認］

（46）　超伝導を応用して磁力誘導で超高速に弾丸を発射する電磁的なレール砲またはレール銃は、「金属性弾丸を発射する機能を有する」ものではあるけれども、火薬の爆発力を応用した「装薬銃砲」ではない。ただし、電磁波砲の中には、電磁的な仕掛けによって筒内の空気を瞬時に膨張させ、それを対象物の破壊のために応用するものがあり、そのようなものの中には「装薬銃砲」または「空気銃」に該当するものがあり得る。

（47）　現行の銃砲刀剣類所持等取締法においては、第二次世界大戦中に盛んに用いられた火炎放射器のような古典的な武器でさえ「銃砲」の範疇に含まれない。あえて皮肉を交えて評価するとすれば、現行法は、ポルトガル人によって種子島に火縄銃が渡来した時代（一五四〇年代ころ）における「武器」という概念に支配され続けているものであり、現代の電子的な仕組みを応用した殺人用具や破壊兵器等を一切考慮に入れておらず、極めて原始的なものであると評価せざるを得ない。なお、「鉄砲」などの火器類が日本国に渡来した正確な年代については諸説あって確定することができないが、それが一六世紀のことであることについては概ね見解が一致している。

（48）　Power grid operators attacked via DDoS

the H: 12 December, 2012

http://www.h-online.com/security/news/item/Power-grid-operators-attacked-via-DDoS-1767170.html［二〇一三年

七月二四日確認］

（49） ICS-CERT Monitor October/November/December 2012 https://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf［二〇一三年七月二四日確認］

（50） 情報セキュリティ担当者の重大な怠慢から本来であれば容易に防御できたはずのサイバーテロを避けることができず、火災や爆発等の事態を招いてしまった場合、当該担当者について業務上失火罪（刑法一一七条の二）が成立する場合があり得ると思われる。

（51） Stuxnet eyed in deadly Iran blast TG Daily (by Trent Nouveau): November 22, 2011 http://www.tgdaily.com/security-features/59781-stuxnet-eyed-in-deadly-iran-blast［二〇一三年七月二四日確認］

（52） 農林水産省農村振興局・農林水産省水産庁・国土交通省河川局・国土交通省港湾局「津波・高潮対策における水門・陸閘等管理システムガイドライン（平成一八年三月）」 https://www.mlit.go.jp/river/shishin_guideline/kaigan/kaigandukuri/suimon/index.html［二〇一三年七月二四日確認］

（53） 道田秀夫・三上　徹・難波田愈「道路交通管制システム」情報処理一九巻六号五五二頁、安達俊朗・渡辺泰男・川見篤史「高速道路交通管制システムの現状とこれから」東芝レビュー五七巻一二号一五頁、高速道路における情報提供の新サービスに関する調査専門委員会「高速道路における情報提供の新サービス」電気学会技術報告一一九〇

（54） 常田信樹・岡田賢一・大島俊哉・渡辺昌夫「都市交通の安全と安定した運行を支える制御管理システム―京阪電気鉄道株式会社の事例―」日立評論八九巻一一号四六頁、国藤　隆・早乙女弘・糟谷直大・前田　徹・渡部　悌「ネットワーク技術による省配線新連動システム「ネットワーク信号制御システム」」同巻同号三八頁

（55） 水道の浄水場では、通常、人間にとっても毒物である塩素やオゾン等の化学物質を用いて消毒が実施されている。これらの消毒用毒物は、所定の量を混入させただけでは人間にとって害はないが（安全基準を守り所定の量を用いている場合に限り正当業務として違法性が阻却され、あるいは、致死量に遠く至らないという意味で不能犯として構成要件該当性が阻却される。）、大量に投入された場合には致死的な結果を招くことが全くないとは言えない。そして、そのような薬物の投入は電子制御され

ているので、その制御を奪いまたはそれを混乱させるなどして大量の薬物投入がなされるようにした場合には、水道毒物等混入の罪（刑法一四六条）が成立し得る。

（56）　服部　大・杉野寿治・横川勝也「上下水道施設の広域・効率化に貢献するシステム技術（特集　水循環と資源再生に向けたソリューション）」東芝レビュー六五巻五号三九頁

（57）　梅崎重夫・池田博康「産業用ロボットの安全性」電子情報通信学会誌八八巻五号三一六頁

（58）　Cyber-attack concerns raised over Boeing 787 chip's 'back door' Guardian: 29 May 2012 http://www.guardian.co.uk/technology/2012/may/29/cyber-attack-concerns-boeing-chip［二〇一三年七月二四日確認］

（59）　オフィスビルやマンションの電源システムをリモートで破壊し非常電源等も機能しないようにした場合、エレベータが停止したまま全く動かなくなってしまうことがあり得る。そのような場合についても、未必的・概括的なものにせよ故意の成立が肯定される限り、間接的な電子的攻撃による監禁罪の成立を認め得ると考える。

（60）　本来、個々のシステムの特性に即して、より具体的に、攻撃の態様と刑罰法令の適用を論ずるべきであるが、その弊害を考慮し、本論文では概括的な指摘だけにとどめることにする。

（61）　詳論は避けるが、例えば、外国から遠隔操作して物理攻撃や偵察活動・諜報活動を実行する飛行型ロボット（攻撃用ドローン）の発着所等を密かに設置した場合、航空法一四六条の適用の可否が問題となり得る。この場合の飛行型ロボットには、ナノテクノロジーの応用によって製造された極めて小型のものや昆虫型のものも含まれる。航空法の適用のある「航空機」は「人が乗って航空の用に供することができる飛行機、回転翼航空機、滑空機及び飛行船その他政令で定める航空の用に供することができる機器」を意味し（同法二条一項）、無人のロボットを含まないが、無人ロボットでも有人のロボットと同様の航空施設や航空保安施設等を要することがあり、それが航空法所定の航空機の飛行の安全（同法一条）の重大な妨げとなることがあり得るからである。ただし、より適切には、全て自律的人工知能コンピュータシステムによって自動的に運用管理される完全な無人施設及び完全な無人航空機であってもそれらに対して航空法の適用があるようにすべく航空法の全面改正がなされるべきである。そして、もし航空法の適用が不適切であるとするのであれば、全く別の立法を考えなければならない。なお、あくまでも一般論だが、人間の存在を必須の前提とする法システムは、既に歴史的産物または博物館の陳列物的存在となりつつある

と言わざるを得ない。

（62） 安全性を高めるようにするとスマートフォン等の製造・管理コストが非常に高いものとなり、一般人が購入可能なレベルを超えてしまうことになる。市販の製品として流通可能な価格帯に押さえようとする限り、情報セキュリティの面での万全性を犠牲にせざるを得なくなると考えられる。そもそも、完全無欠な製品は絶対にあり得ない。

（63） 原子力施設等を破壊したりその制御を奪ったりすることによって当該施設から放射性物質を放出させるような場合だけではなく、何らかの放射性物質を直接に市街地等にばらまいて放射能汚染を発生させるような行為にも適用されることは、当然の前提である。そのような放射性物質は、建築物の非破壊検査やレントゲン医師によるX線検査等のための線源（radiation source）や放射性の蛍光塗料や蛍光インク等として、社会の中に比較的普通に存在する。

（64） 放射能汚染による死亡者の発生を未必的・概括的にせよ認識・認容していた場合には、別途、殺人罪や傷害罪等が成立することは言うまでもない。

（65） 最新の条文の邦訳は、夏井高人「サイバー犯罪の研究（四）―電子計算機詐欺」法律論叢八六巻一号八一頁以下にある。

（66） 関連する古い裁判例等については、吉岡一男「企業秘密と情報財㈠」法學論叢一一七巻三号一頁、同「企業秘密と情報財㈡」同四号一頁が詳しい。

（67） 日本航空電子工業株式会社の株主代表訴訟の第一審判決である東京地裁平成八年六月二〇日判決の掲載雑誌（出典）である。同判決の理由中で刑事事件の主文及び公訴事実の概要が引用されているが、刑事判決の判決書それ自体は未公刊である。

（68） 本論文は、文部科学省私立大学戦略的研究基盤形成支援事業（平成二三年～平成二七年度）による研究成果の一部である。