サイバーセキュリティへの刑事法的対応に関する一考察

星　周一郎

目　次

はじめに——サイバーセキュリティ基本法の制定

Ｍｉｃｒｏｓｏｆｔ Ｗｉｎｄｏｗｓ 95の発売を一つのエポック・メークとした、平成七（一九九五）年以降の二〇年間におけるインターネットの一般社会への急速な普及と普遍化・遍在化の状況に関しては、ここで改めて述べるまでもない。社会生活におけるインターネット環境の普及とそれへの依存度の高まりにより、いまや「インターネット前提社会」とでも評するべき状況が生ずるまでに至っている[1]。そして、それに比例して、そのセキュリティの確保が重大な課題になっていることも、周知のところである。

そのようななか、平成二六（二〇一四）年一一月にサイバーセキュリティ基本法が成立し、すでに全面施行されている。同法二条は、サイバーセキュリティの定義を定めるが、これは、同法の対象領域を、サイバーテロ攻撃のみならず不正送金や内部者による不正行為にも及ばせる、きわめて広い定義といえる[2]。そして、同法に基づき、サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、平成二七年一月に、「情報セキュリティ政策会議」を改組する形で、「サイバーセキュリティ戦略本部」が内閣に設置された。それとともに、基本的施策として、国の行政機関等におけるサイバーセキュリティの確保（同法一三条）、重要インフラ事業者等におけるサイバーセキュリティの確保の促進（一四条）などの諸施策とならんで、「国は、サイバーセキュリティに関する犯罪の取締り及びその被害の拡大の防止のために必要な施策を講ずるものとする」旨の犯罪の取締りおよび被害の拡大の防止（一七条）が、基本施策として明確に位置づけられている。

そこで、本稿では、サイバーセキュリティをめぐる近時の問題状況の一端を概観し、刑事法的な観点から見た対

応のあり方に関して、若干の検討を加えることにしたい。

Ⅰ　サイバー攻撃の動向

サイバー空間のセキュリティに関する現状については、その遍在性や展開の早さもあり、それを包括的に把握することは容易ではない。だが、現時点における一応のものとはいえ、その傾向を見いだすことは、サイバーセキュリティの問題を考えるにあたって不可欠の前提であろう。そこで以下では、そのいくつかに関して、簡単な検討を加えることにしたい。

1　不正送金事犯――技術力を誇るサイバー攻撃から利得を狙うサイバー攻撃へ

近時のサイバー攻撃の特徴の一つとして、自己の技術力を誇るハッカー（クラッカー）タイプの攻撃から、利得を目的とするものへの質的変化を挙げることができる[3]。

インターネットバンキングにかかる不正送金事犯は、その典型であり、件数と被害金額は、平成二四年には六四件・約四八〇〇万円であったのが、平成二五年には一三一五件・約一四億六〇〇万円、平成二六年には一八七六件・約二九億一〇〇〇万円となっている[4]。従来は、ウィルスによる偽の画面やメール等で誘導したフィッシングサイトを利用して不正にパスワード等を入手する手法が主であり、大手都市銀行等の個人口座が狙われることが多く、効果的な防止策として導入の進んだワンタイムパスワード方式を破る手法も登場している。さらに、平成二六年の傾向として、被害の対象が、セキュリティ対策の手の回りにくい小規模な金融機関の法人口座で大きな金額の送金を狙う動きがみられる。すなわち、攻撃側は、常に弱点を探しており、「敵の出方をみて攻撃してくるという、

戦いそのものの様相を呈している」とも評すべき状況にある。[5]

さらに、特に利得目的、金銭目的の犯罪は「費用対効果」の高さから、犯人側では、今後も徹底的な機械化によるサイバー攻撃を図るだけでなく、設計レベルで堅牢化が図られているスマートフォンなどに対抗すべく、システムの脆弱性を狙う手法に加えて、持ち主や運用者自身を騙す、そそのかす、誤作動の誘導などの手口を併用することが予想され、システム的なセキュリティだけでの防止の困難化が推測される旨の指摘もなされている。[6]

2　情報セキュリティへのリスクの甚大化

(1)「利得的な情報」のセキュリティ

サイバーセキュリティは情報セキュリティと密接に関連する部分がある。情報セキュリティとは、①機密性、②完全性、③可用性の三要素を維持することとする概念が一般に援用されている。[7] この領域でも、利得目的でのサイバー攻撃が顕著になりつつある。

その典型が、サーバーへの不正侵入による個人情報等の情報漏えいにかかる事象である。その手口や被害態様は様々であるが、平成二四年頃から目立つようになっているのが、不正アクセスによるＷｅｂサービス利用者の登録情報（個人情報）を狙った攻撃である。その具体例は枚挙にいとまがないが、[8] たとえば、飲食店向け物件情報提供サイトの会員情報四万二八七五件（平成二四年七月）、Ｙａｈｏｏ！ＪＡＰＡＮサーバーへの不正侵入による最大約二二〇〇万件のＩＤ情報（平成二五年四月、五月）、ＯＣＮ・ＩＤのサーバーへの不正アクセスによる最大約四〇〇万件のＩＤ用メールアドレスと暗号化されたパスワード（平成二五年七月）などの大規模な情報流出（または、その可能性のあった）事案が相次いだ。[9]

さらに、アメリカでは二〇一三年以降、小売店のＰＯＳ端末がマルウェアに感染し、不正アクセスにより店舗利

用者のカード情報等約四〇〇〇万件あるいは約六〇〇〇万件の情報漏えいの可能性があるという事象が相次いだ[10]。さらに、二〇一四年八月には、アメリカ二九州で二〇〇以上の病院経営を手がける医療機関から、四五〇万件の患者情報（氏名や住所、生年月日、電話番号、社会保障番号など）の漏えいが発生した[11]。これらは、コンピュータやスマートフォン等による「インターネットに関わる場面」とは一般的に認識されにくい部分も含めた日常生活のあらゆる場面においても、サイバー攻撃の脅威が及びうる状況にすでにあることを示すものといえよう[12][13]。

(2) 政府情報・安全保障情報のセキュリティ

さらに、近年では、政府情報や安全保障という「国家的法益」に関わる情報を狙った攻撃も相次いでいる。標的型攻撃メールは、その典型的な手法である。わが国でこれが知られるようになったのは、平成一七年一〇月に実在の外務省職員のメールアドレスから複数の官公庁にウィルス付メールが届いたという事象が報道されてからであるとされている[14]。

平成二三年九月には、日本、イスラエル、インド、アメリカの防衛産業にかかわる企業に対する標的型攻撃が確認され、そこに三菱重工業が含まれていたことが大きく報道された[15]。また、同年一〇月には衆参両院のコンピューターの、外部からの情報窃取を可能とするウィルスへの感染が判明し、大きな衝撃を与えた。この種のサイバー攻撃はいまも続いており、GSOC（Government Security Operation Coordination team）による政府機関に対する脅威の検知件数は、平成二五年度には約五〇八万件にのぼり、前年度の約五倍に達しており[16]、わが国のみならず、世界各国においてもみられるようになっている[17]。

標的型攻撃メールは、その後も増減を繰り返す状態にあったが、平成二六年下半期に急増し、また手口も年々巧妙化してきている[18]。そして、平成二七年五月には、標的型攻撃メールを端緒として日本年金機構から基礎年金番

号や氏名等約一二五万件の個人情報が不正取得されるなど、収束の気配はみられない。

3　制御システム系への攻撃

以上のようなサイバー攻撃は、いわゆる情報セキュリティだけではなく、社会生活の基盤をなす重要インフラに対する脅威にもなりつつあることにも注意を要する。

その一つが、いわゆる制御システムへのサイバー攻撃である。制御システムとは、センサー、プロセッサー、アクチュエーターを最小構成とし、近時の家電製品、輸送機器、エネルギー機器、素材産業、組立て産業などは、すべて制御システムが要となっている[19]。

従来、サイバー攻撃に関しては、ともすれば仮想世界における情報セキュリティのみが念頭に置かれがちであった。しかし、センサーやアクチュエーターも含み、物理世界までも包括する制御システムのセキュリティでは、環境破壊や爆破も含めた物理的毀損までをも考慮しなければならない。のみならず、ネットワーク経由の攻撃を中心に考えれば足りる情報システムと異なり、制御システムにでは、センサー、アクチュエーター側からの攻撃も視野に入れなければならないなど、考慮すべきセキュリティの枠が格段に広い[20]。

平成二二（二〇一〇）年に問題となったスタックスネット（Ｓｔｕｘｎｅｔ）は、ウラン濃縮工場の遠心分離機の多くを破壊したといわれており、制御システム系のセキュリティの重大性を否応なしにも知らしめることとなった。また、日常生活により密着した場面でも、東日本大震災による重要インフラの停止事象の例からも明らかなように、発電所やガス供給施設、浄水場のコンピューターが攻撃されれば、日常生活にたちまち壊滅的な影響が及ぶリスクが、常に存しているのである[21][22]。

それ以外にも、たとえば、医療機器のセキュリティといった問題も深刻化しつつある。二〇〇九年にはアメリカ

でＭＲＩ装置のウィルス感染が発見され[23]、また、二〇一二年一〇月にはボストンのメディカル・センターで胎児モニター装置がコンピューター・ウィルスに感染するなど、人の生命・健康に直接関わる医療機器に対するサイバー攻撃の可能性も指摘されるようになっている[24]。

4 小括

以上において、近年のサイバーセキュリティの状況を縷々概観してきたが、もちろん、これらは氷山に一角にすぎない[25]。そして、このような状況は、今後ますます加速していくことが予想される。サイバーセキュリティとして、いかなる対応が必要とされるのか、引き続き簡単な検討を加えることにしたい。

Ⅱ サイバーセキュリティ対策の動向

1 サイバーセキュリティ対策の諸施策推進のための体制整備

(1) 内閣官房情報セキュリティセンター（ＮＩＳＣ）の設置

平成一二年に制定された高度情報通信ネットワーク社会形成基本法（ＩＴ基本法）では、高度情報通信ネットワーク社会の形成という、車でいう「アクセル」の側面に重点が置かれていた。もちろん、ネットワーク社会の安全性確保という「ブレーキ」の側面もＩＴ基本法では認識されていたが、高度情報通信ネットワークの安全性・信頼性の確保、個人情報の保護等により、国民が高度情報通信ネットワークを安心して利用するのに必要な措置を講ずることが定められているにすぎなかった（二二条）。

そして、現実の国家的な対策として、情報セキュリティの推進に係る企画および立案ならびに総合調整を行うた

めに、平成一六年一二月のＩＴ戦略本部決定により、内閣官房に、従前の「情報セキュリティ対策推進室」を改組する形で「情報セキュリティセンター（ＮＩＳＣ）」が設置された[26]。ただし、設置根拠は内閣総理大臣決定（「情報セキュリティセンターの設置に関する規則」（平成一七年四月））であり、必ずしも法的根拠が明確化されたとはいえない状況のもとで、情報セキュリティ対策の諸施策が推進されてきた。

(2) サイバーセキュリティ戦略本部の設置とＮＩＳＣの法制化

しかしながら、サイバーセキュリティ対策問題の深刻化に伴い、平成二五年一二月に閣議決定された「国家安全保障戦略」では、サイバーセキュリティの強化が、わが国全体の安全保障戦略の重要な柱の一つとして位置づけられるまでに至る[27]。

そして、サイバーセキュリティ基本法は、政府が、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティに関する基本的計画（「サイバーセキュリティ戦略」）を定めることを規定する（一二条）とともに、その施策の推進のために、内閣にサイバーセキュリティ戦略本部を設置することを定めた（二四条）。これにより、サイバーセキュリティに関する政府の司令塔の設置に、はじめて明確な法的根拠が定められると同時に[28]、ＮＩＳＣも、同法附則二条の施行により、内閣官房組織令に基づき「内閣サイバーセキュリティセンター（ＮＩＳＣ）」へと改組・法制化された。

2 インシデントレスポンスのための体制

情報セキュリティの領域では、脅威とそれに対する脆弱性とが要因となってリスクが発生し、それを攻撃する事象が発生してリスクが現実化することを「インシデント」と称する[29]。そして、そのリスクに対して応急処理を含めた適切な対応をすることを、「インシデントレスポンス（ＩＲ）」と呼んでいる。インシデント発生時の緊急対応

としては、①モニタリング（事象の検知・報告受付）、②トリアージ（事実確認・対応の判断）、③インシデントレスポンス（分析・対処・エスカレーション・連携）、④リスクコミュニケーション（報告・情報公開）という四つの機能から主として構成されるとされている。[30]

そして、以上の四つの機能の全部または一部を有し、インシデント発生時における緊急対応の実施を担う体制のことを「ＣＳＩＲＴ（Computer Security Incident Reponse Team）」という。わが国では、ＩＴ障害を未然に防止するため、関係重要インフラ事業者間の情報共有システムとして、各重要インフラ分野において「ＣＥＰＴＯＡＲ（Capability for Engineering of Promotion, Technical Operation, Analysis and Response）」と、その協議会も組織化されている。また、政府機関に対する攻撃への対応を目的として、ＮＩＳＣが「政府情報機関セキュリティ横断監視・即応調整チーム（ＧＳＯＣ：Government Security Operation Coordination team）」を設立している。[31]また、一般社団法人ＪＰＣＥＲＴコーディネーションセンター（JPCERT/CC）が平成一五年に設立され、インシデントに関する日本国内のサイトに関する報告の受付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言等を、中立的組織として技術的観点から行っている。[32]

３　法執行のための民間との協力体制の必要性・情報共有の重要性

(1)　サイバー空間の法的性質と法執行を含めた官民連携

ＩＴ基本法は、高度情報通信ネットワーク社会の形成にあたって、「民間が主導的役割を担うことを原則」としている（七条）。たしかに、サイバー空間は、産業界や学界などの民間セクターが中心となって構築されてきたという経緯があり、国は補助的な役割を果たすものと位置づけられていた。

これに対して、サイバーセキュリティ基本法一六条は、サイバーセキュリティ施策に取り組むことができるよう

必要な施策を国が講ずる旨を規定する。サイバーセキュリティに国家安全保障の側面が明確に位置づけられた影響もあり[33]、サイバーセキュリティを国主導のものと位置づけている。そして、前述したように、基本的施策の一部として「犯罪の取締りと被害の拡大の防止」という「捜査」という観点も重視されている（一七条）。

もっとも、国が主導で行うといっても、官民一体の連携の必要性は依然として重視されている（一六条）。国も含め、遍在的なサイバー空間のセキュリティに対する単一の組織・体制での対応など、すでに不可能な状況になっていることは論を俟たない。重要なのは、各セクターの有する情報・知見を官民連携のなかで積極的に共有していくことである[34]。

(2) 総合セキュリティ対策会議

警察庁では、平成一三年度以降、警察庁生活安全局長主催の私的懇談会として、「総合セキュリティ対策会議」を設置している。これは、情報通信ネットワークの安全性・信頼性の確保を目的として、情報セキュリティに関する産業界等と政府機関との連携の在り方、特に警察との連携の在り方について有識者等による検討を行うことを目的としたものである。平成一三年一二月の第一回会議以降、現在に至るまで継続している[35]。

そして、平成一三年度の「情報セキュリティ対策における連携の推進について」を嚆矢として、毎年度一ないしは複数のテーマについて検討を行い、毎年報告書を作成している。これは、法執行を含めたセキュリティ関連の政策決定において、重要な意義を有する取り組みであるといえよう[36]。

(3) インターネット・ホットラインセンター

平成一八年に、「インターネット上の違法・有害情報への対応を効果的かつ効率的に推進していくために、広くインターネット利用者から違法・有害情報に関する情報提供を受け付け、一定の基準に従って情報を選別した上

で、警察への情報提供、電子掲示板の管理者等への送信防止措置依頼等を行う団体」として、インターネット・ホットラインセンター（ＩＨＣ）が設置された[37]。これは、平成一七年度総合セキュリティ対策会議での検討結果[38]に基づくものである。

インターネット上におけるフィッシングサイト等の違法・有害サイトについては、それを放置することなく迅速な取り締まりや削除等の対応をすることが、サイバーセキュリティの観点からも重要になる。これら違法・有害情報に対しては、警察によるサイバーパトロールによる発信者の取り締まりや、受信側での情報のフィルタリング等の対応、さらにはプロバイダや電子掲示板の管理者等による違法・有害情報に対する送信防止措置等の対応がなされてきている。しかしながら、インターネットでは膨大な量の情報が日々新たに流通しているのみならず、海外に設置されたサーバーに蔵置されているものがあるほか、コンテンツ自体のコピー、改ざん、削除等が容易であるといった特性もある。

そのため、これらの違法・有害情報への対応としては、広くインターネット利用者の協力を得て違法・有害情報に関する情報を収集することが、より効果的であることになる。すなわち、警察当局の現在の資源だけでは、あきらかに犯罪と思われるものであっても対応しきれない現実があり、他方で、国民から見て信頼できることを前提条件に、民間主導ということも含めて、合理的な官民連携という選択肢も考慮する必要がある[39]。このインターネット・ホットラインセンターも民間主導の官民連携の典型であり、また、インターネット・ユーザーとの協力関係を大切にしている組織であることが、その特徴である[40]。

(4) ＮＣＦＴＡ

また、総合セキュリティ対策会議の平成二五年度のテーマは、「サイバー空間の脅威に対処するための産学官連

携の在り方～日本版ＮＣＦＴＡの創設に向けて～」[41]であった。

ＮＣＦＴＡ（National Cyber-Forensics & Training Alliance）とは、急速に複雑化・国際化するサイバー空間の脅威、特に産業界が直面する脅威への効果的な対処（脅威の特定、軽減および無効化）を可能とするため、産業界、学術機関および法執行機関が保有するサイバー空間の脅威に関する情報を業界横断的かつリアルタイムに収集・分析し、サイバー空間の脅威に共同で対処するための結節点として、一九九七年に創設されたアメリカの非営利団体法人（同法人の資格取得は二〇〇二年）である[42]。創設以来、“One Team, One Goal”を掲げ、産学官が一体となって先制的・包括的な対応を行うことで、サイバー空間の脅威に起因する被害の予防、拡大防止、検挙等に多大な成果をあげ[43]、アメリカ国内外で高い評価を得ており、各国においても同様の取り組みが試みられるに至っている。

総合セキュリティ対策会議報告書は、従来のＣＳＩＲＴやインターネット・ホットラインセンターといった取り組みについて、サイバー空間の脅威への対応に一定の成果をあげているものの、いずれも個別具体の脅威に対して事後的に防御措置を講ずる「受け身」の対応となっているうえ、脅威の質が変化する中でこれに先制的・包括的な対応を行い、脅威の大本を無効化し、以後の事案の発生を止めることは十分にできていないとの認識に立つ。そのうえで、「我が国の脅威の現状及びそれに関する課題を踏まえると、サイバー空間の脅威に関する生の情報や脅威に対処するための技術・知見等を有する産業界と、情報通信技術に係る研究開発等を通じて貢献する学術機関、そして、証拠の差押えや被疑者の逮捕を始めとする捜査権限を行使できる警察等の間で、それぞれが持つサイバー空間の脅威への対処の経験を、その場限り・当事者限りのものとせず、全体で蓄積・共有し、個別的・事後的な受け身の対応ではなく、警察による捜査権限の行使を始めとする先制的・包括的な対応を可能とする産学官連携の新たな枠組み、すなわち、日本版ＮＣＦＴＡを創設する必要がある」旨を報告している[44]。それに基づき、「一般財団法

人　日本サイバー犯罪対策センター」が成立され、平成二六年一一月から業務を開始している(45)。

たしかに、サイバー空間は民間セクターを中心に構成されてきた私的な空間であって、刑事法はなるべく関与すべきではないとする価値判断にも、一定の説得力がある。しかしながら、その一端のみではあるが、本稿で検討したサイバー空間の脅威に関する現状を考えても、「防御」のみでは、往々にして後手の対応にならざるをえず、サイバーセキュリティの確保にとって十分とはいえない状況が生じている。捜査・犯人の検挙という法執行を相対的に重視した情報共有システムの構築が必要なフェーズに至ってきているといえよう(46)。

4　小　括

以上にみてきたように、サイバーセキュリティの対策にとって、刑事法的な対応が重要になってきていることは、否定できない状況にある。そこで、これに対応すべく、刑事実体法的側面と手続法的側面の現状について、引き続き概観することにしたい。

Ⅲ　刑事実体法的な対応

1　不正アクセス禁止罪

刑事実体法的な対応において、サイバーセキュリティにとって重要な機能を果たしているものの一つが、不正アクセス禁止法であることは、改めて述べるまでもないであろう。警察庁の統計によれば、平成二五年中のネットワーク利用犯罪六六五五件のうち、不正アクセス禁止法違反が九八〇件で、一四・七パーセントを占めている(47)。

不正アクセス禁止法は、①不正アクセス行為・情を知ってする助長行為、②他人のＩＤ・パスワードを不正取

得・保管する行為、および③フィッシング行為を処罰対象とする。①に関しては、平成一一年の立法当時から処罰対象であったが、平成二四年の同法改正により、法定刑が引き上げられている。また、②および③に関しては、平成二四年改正により、新たに禁止・処罰の対象とされたものである。

このような不正アクセス禁止法上の処罰類型の保護法益については、必ずしも見解は一致していない。一方では、電気通信回線を通じて行われる電子計算機に係る犯罪の防止を重視し、不正アクセス後になされる侵害行為（詐欺や業務妨害など）の予備的行為を規制するという見解もありうる[48]。だが、このような見解は、予備罪処罰をきわめて例外的に関する現行刑法の基本スタンスには整合しないだけでなく、実態を適切に把握したものとはいえない。むしろ、その保護法益は、アクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与する目的という点、すなわち、「アクセス制御機能に対する社会的信頼」に求めることができる。その際には、不正アクセス行為や、他人のＩＤ・パスワードの不正取得・保管、フィッシング行為等を端的に禁止する趣旨と、すでに検討した、現今のサイバーセキュリティ状況を踏まえるのであれば、コンピューター・ネットワーク全体に対する社会の信用にとどまらず、それにより実現されるサイバー空間の秩序そのものと、それに依拠した社会の安全とを保護法益とする公共危険犯と解すべきであろう[49]。

なるほど、法益侵害原理を重視し回顧的・謙抑的処罰を何よりも重視してきた従来の刑法理論における予備罪処罰のあり方からすれば、不正アクセス行為等を端的に処罰行為とすることは、「きわめて異例」であるとはいえよう[50]。しかしながら、サイバーセキュリティが、社会生活の根幹にかかわる問題になっている以上、そこに、インターネット普及前の社会状況では認められなかった、新たな保護法益が生じていると評すべきである[51]。そしてそれは、影響（リスク）の甚大化、それの及ぶ範囲の広範性・瞬時性（リスクの拡散性）にかんがみれば[52]、新た

な公共危険犯としての理解を根拠づける事情として位置づけられるように思われる。

2　不正指令電磁的記録に関する罪（ウィルス罪）

また、周知のように、平成二三年の刑法一部改正により、刑法典に「第一九章の二　不正指令電磁的記録に関する罪」が新設され、不正指令電磁的記録作成等の罪（一六八条の二）および不正指令電磁的記録取得等の罪（一六八条の三）が規定された。

コンピューター・ウィルスの被害に関しては、一九九〇年代からすでに問題となっていたが、従来はその作成等自体を直接処罰する法律はなかった。それゆえ、当該ウィルスの具体的内容により、電磁的記録不正作出・毀棄罪や、不正アクセス禁止法等による対処[53]のほか、いわゆる「イカタコ・ウィルス」をインターネット経由で被害者に感染させた行為について、ハードディスクの本来的効用（読み出し機能と書き込み機能）の喪失と一般人では容易に原状回復できない点をとらえて器物損壊罪の成立を認める（東京高判平成二四年三月二六日東高刑時報六三巻一＝一二号四二頁[54]）、あるいは、同一の被告人による、大学同級生の顔写真やアニメのイラストを使用した「原田ウィルス」を被害者に感染させた行為について、著作権法違反の罪と名誉毀損罪の成立を認める（京都地判平成二〇年五月一六日公刊物未登載）といった苦しい対応[55]に終始せざるをえなかった[56]。しかしながら、欧州評議会のサイバー犯罪条約では、コンピューター・ウィルスの作成等の処罰を明示的に求めており、条約締結のための罰則整備という形で、前述の改正が行われたものである[57]。

コンピューターが今日の国民の日常生活において果たす役割を機能に鑑みると、ウィルスソフトの作成自体によって、コンピューター利用に対する不安が生じ、インターネット環境全体への信頼性が減じられることになる。社会は、プログラムを信頼して情報処理等をしているのであり、不正指令電磁的記録の作成等の処罰は、そのような

社会的信頼を保護法益としたものと理解されるが[58]、前述のように公共危険犯性も認められよう。

もっとも、不正指令電磁的記録に関する罪の立法にあたっては、「構成要件の明確性」が重要な争点となった。その一つが、当初平成一七年の立法提案時にはなかった、「正当な理由がないのに」（正当な理由の不存在）という要件の追加である。これは「違法に」という意味であり、ウィルス対策ソフトの開発・試験等を行う目的でウィルスを作成し、他人の承諾を得て動作させるような場合、「人の電子計算機における実行の用に供する目的」がないため構成要件該当性は否定されるが[59]、その趣旨を一層明確化する趣旨として同要件が追加されたものである[60]。

他方、それ以上に争われたのがバグの問題である。技術系の側からすれば、「プログラミングには必然に近くバグが発生する」ものである以上、そのバグにウィルス的な機能が備わってしまうと直ちに処罰されるのではないか、という疑念も一方では生じうる。もちろん、不正指令電磁的記録に関する罪は故意犯・目的犯である以上、過失によるバグについては構成要件の主観面が充足されないことになるが、「バグがあることを何度も指摘されても放置したら、故意や目的が認められることになりかねない」旨の疑念が強く指摘されたのであった。しかし、不正指令電磁的記録作成・取得等の行為の当罰性自体には、大方の理解が得られているのである。そして、条文の文言は抽象的なものにとどまらざるを得ない性質をもっている以上[61]、一定程度の価値判断を含んだ実質的構成要件解釈を採用し、法律家の側と技術者の側等との相互理解により、具体的に処罰に値する場合を類型化することで、妥当な処罰範囲を導く解釈のあり方を検討していくことこそが必要となる[62]。

3　情報セキュリティと刑事法

すでに論じたように、近時は利得目的でのサイバー攻撃も多い。そして、不正送金等の事案では、その行為対象や対象場面によって、不正アクセス禁止法以外にも、電子計算機使用詐欺罪や犯罪収益移転防止法違反などによる

立件がなされているようである。[63]

他方で、それと並んで増加しつつあるのが、データベース等に蓄積された情報の不正取得等を目的とするサイバー攻撃であり、端的に「情報セキュリティ」に関わる態様のものといえよう。情報セキュリティに関連する法分野は多岐にわたるが、刑事法的観点からは、不正に取得等された情報が、被害者にとって不正競争防止法にいう「営業秘密」（同法二条）にあたるのであれば、営業秘密侵害に関する罪の成立が認められることになる。同罪については、仙台地判平成二一年七月一六日（特許ニュース一二六二一号一頁）[64]を嚆矢として、いくつかの適用例が見られるようになった。そして、横浜地裁川崎支判平成二四年九月二〇日（公刊物未登載）[65]、名古屋地判平成二六年八月二〇日（ＬＥＸ／ＤＢ：二五五〇四七一九）、東京地判平成二七年三月九日（ＬＥＸ／ＤＢ：二五五〇六一六一）などは、いずれも内部者による事案であるが、営業秘密の記載された電子ファイルをコピーして外部記憶媒体（ＣＤ―Ｒ、外付けハードディスク）に記録するという手口であり[66]、当然のことながら、このような電子ファイルの不正取得は、外部からのサイバー攻撃等によっても十分に行いうるものである。

さらに、平成二七年に国会に提出された個人情報の保護に関する法律の改正案では、前述のベネッセ事件を契機として、個人情報データベースの取扱者らが、不正な利益を図る目的で個人情報を提供または盗用する行為を処罰対象とする「データベース提供罪」の新設が提案されており、今後の動向が注目される。

しかしながら、さらにすすんで、「情報窃盗」一般を刑事処罰の対象にすることの是非も問われ続けている。情報（データ）の不正取得等の処罰は、昭和六二年の電磁的記録・電算機使用関連犯罪を新設する刑法の一部改正でも積み残しとなった[67]。だが、サイバーセキュリティの重要性だけでなく、情報化社会となった今日の状況を踏まえれば、「情報窃盗」の処罰立法の必要性も依然として主張されており[68]、今後、検討が必要となろう。

Ⅳ　刑事手続法的な対応

1　平成二三年刑事訴訟法改正

サイバー空間を舞台とした犯罪の増大は、手続法の側面、すなわち、従来の刑事手続上の諸概念に対しても大きな影響を及ぼしている。

従来、文書の形式で記録・保存されていた情報は、現在は電磁的記録媒体等で記録・保存されることが多い。電磁的記録は大量の情報を容れることができ、文書類のような可視性・可読性もなく、情報の処理・加工・消去等も容易であるなど、昭和二三年制定の現行刑事訴訟法の捜索差押え手続では、必ずしも適切な対応ができないことも多かった[69]。

そこで、平成二三年の刑事訴訟法改正により、電磁的記録の捜査に関し、電気通信回線で接続している記録媒体からの複写（九九条二項、二一八条二項）、記録命令付差押え（九九条の二）、電磁的記録にかかる記録媒体の差押えの執行方法（一一〇条の二、二二二条一項）、保全要請（一九七条三項ないし五項）、協力要請（一一一条の二、一四二条、二二二条一項）などの規定が整備された[70]。

2　デジタル・フォレンジックの重要性

デジタル・フォレンジックとは、一般的には、コンピューター等を利用してデジタルの世界の証拠性を確保し、法的問題の解決を図る手段をいう[71]。より厳密に、「インシデント・レスポンスや法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一

連の科学的調査手法・技術を言う」とする定義もある[72]。デジタル・フォレンジックは、現在、犯罪捜査や内部不正の調査への対応のみならず、インシデントレスポンス、さらには、いわゆるｅディスカバリ（電子的証拠開示）といった場面でも問題とされるようになっている[73]。

他方で、捜査関係用語として考えた場合、デジタル・フォレンジックは科学的捜査手法の一つと位置づけられ、警察では「犯罪の立証のための電磁的記録の解析技術およびその手続」という意味で使用されることが多い[74]。そこで、とりわけ、捜査分野におけるものという観点に特化して、「デジタル機器類（独立した電磁的記録媒体を含む。）の内部に残された電磁的記録の中から、証拠になり得るものを、可能な限り、そのままの状態で、収集・取得し、保全し、解析することで、捜査・公判の各段階における証拠収集手続、証拠能力及び証拠の証明力に対する疑義を可及的に低減し、事案の解明と適正な事実認定の実現に資することを目的として行われる捜査活動」とする定義も提案されている[75]。

このデジタル・フォレンジックも、近年重要性を増している。警察庁情報技術解析課が実施する情報技術解析支援の平成二五年の実施件数は二万二一九七件（平成一六年の約三・八倍）であり、平成二一年以降二万件を超える水準で推移する一方、電磁的記録の解析総容量は五・四ペタバイト（平成一八年の約一二倍）で、増加の一途をたどっている[76][77]。

このようなデジタル・フォレンジックの刑事手続に及ぼす影響についても、今後検討の必要がある。捜査という観点からすれば、記録媒体の大容量化なども含め、デジタル証拠の発見・収集自体が困難化しつつある一方、指掌紋の採取・照合やＤＮＡ型鑑定のような標準的手続（およびそのガイドライン）が確立していない、といった問題点も指摘されている[78]。さらに捜査・公判の構造との関係では、原本保管の重要性や押収・保全プロセスの記録の

重要性など[79]、いわゆる、証拠の真正性・同一性の立証に関する証拠管理の継続性[80]に関わる問題に関連して、人材の育成だけでなく、手続的な整備等が必要となることも考えられよう。

Ⅴ　今後の課題

1　サイバー攻撃・サイバー犯罪の予防と法的対応

刑事的な法執行の必要性が重要になってきているといっても、もちろん、ひとたび事象が生じた場合、その影響が甚大かつ深刻なものになりうるサイバー攻撃・サイバー犯罪に関して、その予防が重要課題であることに変わりはない。そのため、情報セキュリティのための取り組みについて、今後もより一層の推進が求められることはいうまでもない。

ただし、この未然防止という観点については、刑事実体法および行政的措置も含めた手続法の両面においても対応の必要性があるように思われる。

刑事実体法的な側面としては、先に述べた不正アクセス禁止等の罪、および不正指令電磁的記録に関する罪の公共危険犯的理解という形で顕在化する。実害発生前の未遂および予備段階での処罰自体、結果発生の危険性を処罰根拠とするが、それに加えて、先にものべたように、これらの罪では、その影響力の不特定的な拡大という意味において、公共の危険性・社会的法益の侵害性を伴うものである。さらに、それに犯罪の未然防止を求める社会的要請が加わり、従来の法益侵害原理に基づく回顧的な処罰からすれば早期段階とも評しうる処罰を根拠づけるものと解される[81]。もっとも、このような性質を有するあらゆる危険を、すべて処罰対象とする必要があるかは別途の検

討が必要となり、従来の刑法解釈論の根幹であった侵害原理・法益保護原則のみならず、処罰の必要性と被侵害利益との比較考量、コストや自由の配分といった比例原則によることにより、処罰に値すべき場面を選択していくことが必要となるであろう[82]。

他方、手続法的側面についてみると、捜査環境の整備による犯罪予防効果に加えて、現実世界での犯罪予防の権限を、サイバーにおいて認めるべきであるとする見解もある。すなわち、現実世界では、たとえば、警察官職務執行法五条は、人の生命、身体に危険を及ぼし、財産に重大な損害を与える犯罪が急迫している場合には、警察官にそれを制止する権限を与えている。これと同じように、重大なサイバー攻撃が進行している際に、警察官や関係者が状況を把握し急迫不正の侵害に及ぶような通信を直ちに遮断できる根拠を認めるような法制の検討が考えられるとする問題意識である[83]。

ストーカー規制法や児童虐待防止法などをみるまでもなく、近時の世論は、犯罪の未然防止をより一層強く求めてきている。そして、法理論としても、そのような要請に対して、どのような対応をすべきかが問われる時代になってきているといえよう[84]。もちろん、次で言及する「通信の秘密」やその他利害関係者の権利の保護といった問題など、現実世界と直ちに同列に論ずることはできないが、サイバー上のリスクの高まりを背景にすると、そのような検討が必要となってくることが考えられる。

2　通信履歴（ログ）の保存――「通信の秘密」の意義と範囲

また、サイバー攻撃（のみならずネットワーク利用犯罪等）への対処において、その行為者を特定するには、ネットワーク上の通信履歴（ログ）が必要となる。これは、従来型犯罪における現場遺留物、目撃証言や防犯カメラ映像などに相当するものであろうが、ネットワークにおいては、唯一・絶対な証拠であり、ログがなければ、被疑

者の特定はほぼ不可能となるという特質がある。そのため、ログの保存は、以上に縷々述べてきたサイバーセキュリティ対策が「画餅」に陥らないようにするためにも不可欠である[85]。

ところが、ログの保存に関しては、周知のように、憲法二一条二項の定める「通信の秘密」との関係が夙に問題とされている。電気通信事業法四条一項は、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない」とする。そして、総務省の「電気通信事業における個人情報保護に関するガイドライン（平成一六年総務省告示第六九五号。最終改正平成二五年総務省告示第三四〇号）」一三条一項は、「電気通信事業者は、通信履歴（利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のものをいう。以下同じ。）については、課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な場合に限り、記録することができる」と定める。そして、総務省による同ガイドラインの解説[86]において、①「通信履歴は、通信の構成要素であり、電気通信事業法第四条第一項の通信の秘密として保護され」、通信履歴の記録も通信の秘密の侵害に該当しうるが、課金等の業務の遂行上必要な場合には正当業務行為として違法性が阻却されるとし、また、②記録した通信履歴は、録目的に必要な範囲で保存期間を設定することを原則とし、保存期間が経過後は速やかな消去を要するが、法令の規定による場合その他特別の理由がある場合には例外的に保存し続けることができると考えられ、自己または第三者の権利を保護するため緊急行為として保存する必要がある場合は、その他特別な理由がある場合として保存が許される、とする見解が示されてきた。

しかしながら、このような解釈に対しては、近時、重要な疑問が提示されるようになっている。たとえば、電気通信事業法四条一項にいう「通信の秘密」と二項にいう「他人の秘密」を峻別すべきとする見解も有力に主張されている。論者は、前者は、「通信内容」に関わるもので、通信傍受法による場合以外には絶対的に保護されるが、

通信内容はログには含まれず、ログそのものは通信内容以外の付帯的なメタ情報であり、二項にいう「他人の秘密」として、より緩やかな規制に服するべきものであり、ログの保存は、そのような文脈で考えるべきであると指摘する[87]。コンピューター通信の場合には、①接続先のサーバーに保存されている接続ログ（アクセスログ）と、②接続者（インターネットユーザー等）がインターネットサービス・プロバイダー（ＩＳＰ）を経由する場合に認証サーバーに保存される認証ログとがある。このうち、犯罪等が行われた時間に当該ＩＰアドレスを誰（契約者）に割り当てていたのかは、認証ログを確認しなければならない。この認証ログが、憲法二一条二項や電気通信事業法四条一項にいう「通信」に関するものとすることにも疑問の余地があるが[88]、一方で、通信の秘密に関する先の指摘をも踏まえつつ、他方で、サイバーセキュリティ対策において刑事法的な対応も重要な要素と位置づけるのであれば、少なくとも認証ログについては、その保存には合理的理由があり、それに関する法整備等を行う必要がある[89]。

紙数の関係もあり詳細な検討は別の機会に譲ることとしたいが、現在の電気通信事業法の「通信の秘密」に関する議論は、電電公社・ＫＤＤにより電信電話通信が独占的に行われてきた時代からほとんど変わっていない。しかしながら、近時にわかに活性化している通信の秘密をめぐる解釈論に関して、「憲法上の通信の秘密の範囲を広く理解することが現在のインターネット環境との関係で適切かどうかという問題提起として受け止めるならば、その指摘には耳を傾けるべきものが多分に含まれているように思われる」とする指摘[90]は、サイバーセキュリティのあり方を考えるうえで、きわめて重要である。

3　事後追跡可能性の確保の意義

平成二四年に生じた遠隔操作ウィルス事件で、ＩＰ等にもっぱら依拠した誤認逮捕の判明後、平成二五年二月の

犯人検挙に直接結びついたのは、犯行声明を著名観光地の地域猫の首輪にくくりつける犯人を撮影した防犯カメラ映像であり、翌年四月に否認を続ける被告人が自白に転じたのも、保釈中の被告人が「真犯人からのメール」を装ったメールを送信した際の捜査員による行動確認を契機とするものであった[91]。

通信履歴（ログ）保存等に関しては、国家権力によりインターネット上の監視がなされ、国民監視等で優越的な地位に立つことにつながる、といったイメージで語られることもある。しかし、右の例からも示唆されるように、ＩＳＰの自主的な対応により一定程度のログの保存がなされている現状においても、そのような現実が生じているとはいえない。むしろ、サイバー空間は、犯罪者に著しく有利で犯罪対策には著しく不利な環境になっているのが現状であるとの指摘もなされている[92]。それは、サイバー空間の変化・展開の著しさ、サイバー犯罪の拡大と技術的巧妙化の速度に現実の捜査力が追随できないという面だけでなく、主として現実世界を念頭に置いて制定・解釈されてきた現行法の限界の現れでもあろう。通信の秘密をめぐる解釈論が近時にわかに活発化しているのも、その文脈において理解できるものである。

捜査における事後追跡は、犯罪が生じてから行うものであって、現実世界では、これまで当然に行われてきたものである。それはサイバー空間であっても同じであり[93]、人の行動等の常時監視とは質的に相違するものである。それどころか、行政法であれ私法であれ、法の支配を実効たらしめるためには証拠に基づく事実認定が必須であるが、それは事後追跡可能性の存在を前提とするものである。「インターネット前提社会」においては、サイバー空間における事後追跡可能性の確保は、ひとり刑事法の問題にとどまるものではない[94]。

さらに、国境のないサイバー空間において、日本の法制がセキュリティ・ホールの要因となることは許されない。日本のサーバー等を踏み台にすることで、追跡可能性を遮断してしまうと、サイバーセキュリティに対する国

際的な取組みにとっても著しい問題となり、国際協調の観点からいっても許容されることではなかろう。

Ⅵ　むすびにかえて

以上、サイバーセキュリティに対する刑事法的対応のあり方について思いつくところを縷々述べてきたが、結局は散漫な内容の羅列にとどまってしまった。それは、著者の理解・検討の不足に起因するものであるが、サイバー空間の状況の変化の早さや遍在性のゆえに、現時点における体系化的把握が困難な状況にあることも、また事実である。

とはいえ、サイバー空間の出現は、従来の社会構造・価値観を大きく変化させるものであり、それに伴い、「社会の病理」である犯罪も、その様相を大きく変化させている。もちろん、変化が早く著しいといっても、旧来の価値基準を一気に置換するものではなく、連続性・漸次性をもった変化である以上、サイバーセキュリティのあり方の検討においても、従来の法原則や法的価値観との整合性を図る必要はある[95]。しかしながら、サイバーセキュリティ対策については、「入口対策だけで攻撃を防ぎきるのは困難である」[96]ことがほぼ共通認識となるに伴い、刑事法的対応の必要性も大きくなり、法理論にもそれに応じた対応が求められている。さらには、被害の未然防止の要求という近時の流れも、当然考える必要がある。以上を踏まえたうえで、今後、個別の観点についてさらに検討を加えていくことにしたい。

前田雅英先生は、昭和五〇年九月に当時の東京都立大学法学部助教授に就任された後、実に四〇年近くにわたり、東京都立大学／首都大学東京から、わが国の刑事法・刑事実務をリードされてきた。そして、昭和五七年出版

の『可罰的違法性論の研究』は、一貫して実務的観点・実践性を重視する構成要件論・違法性論を提示するものであったが、その理論は、本稿でも取り上げた不正指令電磁的記録に関する罪の立法にとっても、きわめて重要な役割を果たすものとなっている。また、前田先生は、夙に、またその最終講義においても、「事実が変われば刑法（解釈）も変わる。それを最後に決めるのは国民の規範意識である」ことを強調された。本稿でインターネットの社会一般への普及の年として設定した平成七年から今年で二〇年が経過するが、これは前田先生の在職期間のちょうど半分にあたる。サイバー空間の出現とそれに伴う社会構造の変化は、先生の理論がその真価を発揮する場を提供するものでもあった。

サイバーセキュリティに関する刑事法的課題の検討としては、あまりにも拙いものではあるが、今後の自らの研鑽を誓いつつ、小論をもって前田雅英先生のご退職をお祝いすることとしたい。

（1）　村井純「インターネット前提社会の出発によせて」同ほか『インターネットの基礎――情報革命を支えるインフラストラクチャー』（二〇一四年）一頁以下。

（2）　岡村久道「サイバーセキュリティ基本法の解説」行政&情報システム五一巻一号（二〇一五年）四九頁。これは、後述するように、サイバーセキュリティが問題となる領域が非常に広範にわたることの反映であると理解できよう。

（3）　羽室英太郎『情報セキュリティ入門〔第三版〕』（二〇一四年）一五頁。これは、平成一七年頃から見られた変化である。西本逸郎「サイバー攻撃と防御の基礎」土屋大洋監修『仮想戦争の終わり――サイバー戦争とセキュリティ』（二〇一四年）三三頁以下。

（4）　警察庁『平成二六年中のインターネットバンキングに係る不正送金事犯の発生状況等について』（二〇一五年）一頁〈http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf〉。

（5）　坂明＝四方光「サイバー犯罪とは何か」土屋大洋監修『仮想戦争の終わり――サイバー戦争とセキュリティ』（二〇一四年）一四二頁―一四三頁。

（6）　西本・前掲注（3）論文五四頁―五六頁。

（7）　このような観点に基づき、情報セキュリティ法の体系化を提唱するものとして、岡村久道『情報セキュリティの法律〔改訂版〕』（二〇一一年）。

（8）　その概要をまとめて一覧に供しているものとして、たとえば、独立行政法人情報処理推進機構（ＩＰＡ）編『情報セキュリティ白書二〇一三』（二〇一三年）一八頁、同編『情報セキュリティ白書二〇一四』（二〇一四年）一六頁―一七頁。

（9）　比較的近時においても、ＪＡＬ（日本航空）顧客情報システムへの不正アクセスによる四一三一名分のＪＡＬマイレージバンクの会員情報が外部に流出した事案などが生じている。日本航空・顧客情報漏えい問題に関する独立役員検証委会『検証報告書（要約）』（二〇一五年）一頁以下〈https://www.jal.co.jp/info/other/150122.pdf〉。

（10）　二〇一三年一二月の小売り大手「Ｔａｒｇｅｔ」のＰＯＳ端末（カード情報約四〇〇〇万件）〈http://www.itmedia.co.jp/enterprise/articles/1312/20/news078.html, http://www.itmedia.co.jp/enterprise/articles/1401/17/news036.html〉、および二〇一四年九月の大手ホームセンター「Ｈｏｍｅ　Ｄｅｐｏｔ」のＰＯＳ端末（カード情報約六〇〇〇万件）〈http://blog.trendmicro.co.jp/archives/9890〉。

（11）　「コミュニティ・ヘルス・システムズ」の事案であり、中国からのサイバー攻撃によるものであると報じられている〈http://jp.reuters.com/article/jpUSpolitics/idJPKBN0GJ01V20140819〉。

（12）　また、著作権侵害事犯ではあるが、二〇一四年一一月には、アメリカの映画会社が大がかりなサイバー攻撃を受け、未公開のコメディー映画などのファイルがインターネット上に流出する事態も生じ、当該映画でコメディーの対象とされた国による関与の可能性が指摘されている（産経新聞二〇一四年一二月二〇日付報道などによる）。

（13）　なお、情報流出事案に関しては、それが被害企業にとって営業秘密の侵害にあたる場合も多く、内部者による情報の流出事案も頻発している。たとえば、平成二六年七月に表面化したベネッセコーポレーションの顧客情報流出事件では、最大二〇七〇万件に及ぶ氏名・住所・性別・生年月日等の個人情報の漏えいがあったが、これは、データベース管理委託先の下請会社の派遣ＳＥによるものであったことが報じられている。

（14）　ＩＰＡ編『情報セキュリティ白書二〇一二』（二〇一二年）一二頁。

（15）　http://internet.watch.impress.co.jp/docs/news/20110920_478766.html. 詳細な分析として、たとえば、独立行政法人情報処理推進機構『標的型サイバー攻撃の事例分析と対策レポート』（二〇一二年）三頁以下〈http://www.ipa.go.jp/files/000024536.pdf〉。

（16）　情報セキュリティ政策会議『サイバーセキュリティ政策に係る年次報告（2013年度）』（二〇一四年）八頁〈http://www.

nisc.go.jp/active/kihon/pdf/jseval_2013.pdf>。

（17）総務省『平成二四年版情報通信白書』（二〇一二年）一四六頁以下。

（18）警察庁『平成二六年中のサイバー空間をめぐる脅威の情勢について』（二〇一五年）二頁以下<https://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf>。

（19）新誠一「制御システムのセキュリティ――重要インフラの制御システムを狙うサイバー攻撃にいかに対処するか」土屋大洋監修『仮想戦争の終わり――サイバー戦争とセキュリティ』（二〇一四年）七五頁。

（20）同右七六頁。

（21）制御システム系のインシデント報告は、平成二二（二〇一〇）年の三九件に対し平成二五（二〇一三）年は二五六件へ、脆弱性報告件数も平成二二年の四一件から平成二五年には一八一件へと、増加をみている。

（22）なお、二〇一三年三月に韓国で放送局、金融機関、保険会社のコンピューターに一斉に障害が発生するという深刻な事態が生じており、韓国政府は、これを、社会混乱の惹起を目的とした北朝鮮からのサイバー攻撃であると結論づけた。ＩＰＡ編・前掲注（8）『情報セキュリティ白書二〇一三』二二頁。そして、この攻撃に用いられたマルウェアは、同時期に日本でも発見されており、わが国にとっても決して「対岸の火事」ではない。

（23）二〇一五年三月一六日付読売新聞による。なお、同報道による「医療ハッカソン」の取り組みも参照。

（24）ＩＰＡ編・前掲注（8）『情報セキュリティ白書二〇一四』一四五頁。また、深津博ほか「重要インフラ、特に医療分野におけるサイバーセキュリティ」警察政策一七巻（二〇一五年）二一一頁以下〔深津博〕参照。

（25）なお、独立行政法人情報通信研究機構（ＮＩＣＴ）の調査によれば、国内外から日本の政府機関や企業などに向けられたサイバー攻撃関連の通信は、平成一七年には約三億一千万件であったのが、平成二六年には約二五六億六千万件となり、前年の一二八億八千万件からでもほぼ倍増し、サイバー空間の攻撃が激しさを増していることが示されている（二〇一五年二月一七日付産経新聞ほか各報道による）。

（26）サイバーセキュリティと経営戦略研究会編『サイバーセキュリティ』（二〇一四年）一一〇頁〔武智洋〕。

（27）谷脇康彦「サイバーセキュリティは全世界共通の課題――わが国の対策と戦略、ＮＩＳＣの役割」時評五六巻六号（二〇一四年）一〇〇頁など。

（28）岡村・前掲注（2）論文五二頁。

（29）岡村・前掲注（7）書五頁。

（30）佐々木良一監修『デジタル・フォレンジック事典〔改訂版〕』（二〇一四年）三八二頁〔野崎周作〕。

(31) 羽室・前掲注（3）書三〇八頁。
(32) ＪＰＣＥＲＴコーディネーションセンター『ＪＰＣＥＲＴ／ＣＣについて』<https://www.jpcert.or.jp/about/>。
(33) 岡村・前掲注（2）論文五二頁。
(34) 西本・前掲注（3）論文六〇頁以下など、その指摘はすでに多くなされている。他機関連携の具体例も枚挙に暇がないが、たとえば、重要インフラの制御システム系のセキュリティに関して、平成二四年設立の「制御システムセキュリティセンター（Control System Security Center：ＣＳＳＣ）」が、産官学の連携によるセキュリティ構築のための活動を行っている。新・前掲注（19）論文九六頁。
(35) 同会議の委員長は、平成一三年度以降一貫して前田雅英教授が務めており、テーマに応じて、ＩＴ事業者、大学教員、弁護士、マスコミ関係者、関連事業者等の広範な層が参加する形で開催されている。
(36) 坂＝四方・前掲注（5）論文一六九頁参照。
(37) インターネット・ホットラインセンター『ホットラインセンターのご案内』<http://www.internethotline.jp/about/hotline.html>。
(38) 平成一七年度総合セキュリティ対策会議報告書『インターネット上の違法・有害情報への対応における官民の連携の在り方について』（二〇〇六年）<http://www.npa.go.jp/cyber/csmeeting/h17/pdf/pdf17.pdf>。
(39) 前田雅英「ネット社会の課題―サイバー空間に潜む危険と安全対策―」警察政策一二巻（二〇一〇年）一四頁。
(40) 坂明「サイバー警察」関根謙一ほか編『講座警察法第二巻』（二〇一四年）五三六頁。活動状況について、隈良行「インターネット・ホットラインセンターの紹介」研修七〇六号（二〇〇七年）二七頁以下。
(41) 平成二五年度総合セキュリティ対策会議報告書『サイバー空間の脅威に対処するための新たな産学官連携の在り方～日本版ＮＣＦＴＡの創設に向けて～』（二〇一四年）<http://www.npa.go.jp/cyber/csmeeting/h25/pdf/h25_honpen.pdf>.
(42) 同右二頁。
(43) マリア・ヴェロ（渡辺幸次編集）「サイバー空間の脅威に対処するための連携の在り方」警察学論集六七巻五号（二〇一四年）四九頁以下。
(44) 平成二五年度総合セキュリティ対策会議報告書・前掲注（41）書四頁。
(45) 一般財団法人日本サイバー犯罪対策センター『サイバー犯罪対策新組織「日本サイバー犯罪対策センター（ＪＣ3）」の業務開始』（二〇一四年）<https://www.jc3.or.jp/media/pdf/pressrelease.pdf>
(46) 拙稿「サイバー空間の脅威に対する情報共有組織の意義」警察学論集六七巻五号（二〇一四年）一〇一頁以下

(47) 警察庁『平成二五年中のサイバー犯罪の検挙状況等について』（二〇一四年）一頁 <http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf>。

(48) 渡邊卓也「不正アクセス罪の罪質とその立法動向」Ｌａｗ＆Ｐｒａｃｔｉｃｅ七号（二〇一三年）一一五頁以下参照。

(49) 以上の詳細に関しては、拙稿「公共危険犯の現代的意義」刑法雑誌四八巻二号（二〇〇九年）二〇一頁。

(50) 松原芳博「国民の意識が生み出す犯罪と刑罰」世界七六一号（二〇〇七年）五五頁。

(51) なお、前田雅英「不正アクセス法制の刑事法学的意義」警察政策二巻一号（二〇〇〇年）二三一頁以下参照。

(52) 谷脇康彦「サイバーセキュリティ戦略の最近の動向」日本データ通信一九八号（二〇一四年）二頁参照。さらに、「リスクのグローバル化」もみられ、法執行のあり方について、困難な問題を生じさせている。また、サイバー犯罪の特徴として、「匿名性・隠匿可能性」「瞬時性・大量性・空間無限定性」「分散性」「情報性」「専門性・技術性・『進化性』」を指摘する見解もある。四方光「わが国におけるサイバー犯罪の現状と若干の犯罪学的及び刑事政策学的考察」法学新報一一七巻七＝八号（二〇一一年）四一五頁以下。

(53) 荒川雅行「ウィルス作成罪」法学教室三七四号（二〇一一年）二頁。

(54) 第一審（東京地判平成二三年七月二〇日判タ一三九三号三六六頁）に対する評釈として、園田寿「判批」甲南法務研究八号（二〇一二年）一〇三頁、浅田和茂「判批」新・判例解説Ｗａｔｃｈ（法学セミナー増刊）一一号（二〇一二年）一三五頁、森住信人「判批」刑事法ジャーナル四一号（二〇一四年）二一一頁。

(55) 加賀谷伸一郎「コンピューターに感染する不正プログラムの現状」罪と罰四八巻四号（二〇一一年）四五頁以下参照。

(56) なお、石井徹哉「サイバー犯罪と刑法上の課題」犯罪と非行一六八号（二〇一一年）六一頁以下参照。

(57) 山口厚「サイバー犯罪条約に関連した刑法改正案」Ｌａｗ＆Ｔｅｃｈｎｏｌｏｇｙ二六号（二〇〇五年）七頁、佐伯仁志「サイバー犯罪条約への実体法上の対応」ダニエル・フット＝長谷部恭男編『メディアと制度』（二〇〇五年）八七頁など。その後の立法の経緯に関して、杉山徳明＝吉田雅之「『情報処理の高度化等に対処するための刑法等の一部を改正する法律』について」警察学論集六四巻一〇号（二〇一一年）三頁以下など。

(58) 前田雅英『刑法各論講義〔第五版〕』（二〇一一年）五五六頁。

(59) もともと、ウィルス対策ソフトの開発・試験等を行う目的でのウィルスの故意使用を処罰対象としないことは、サイバー犯罪条約でも明確に要請されているところであり（六条二項）、また、当初の条文案でも適切な対応はなしうるものであった。今井猛嘉「実体法の視点から」ジュリスト一四三一号（二〇一一年）六八頁。

(60) 杉山＝吉田・前掲注（57）論文九頁。

(61) 条文に一定程度抽象的な部分が残らざるをえないという問題は、すべての犯罪類型にとって多かれ少なかれ妥当するものである。たとえば、殺人罪の客体である「人」に関しても、「いつから胎児は人になるのか」「脳死状態の者はまだ人か」といった価値判断を含んだ実質的解釈が不可避なのである。実質的構成要件概念について、前田雅英『可罰的違法性論の研究』（一九八二年）四七五頁以下。

(62) 前田雅英「サイバー犯罪の現状と対策――不正アクセスから国民を守る――」警察政策一四巻（二〇一二年）一四頁以下。やや文脈を異にするが、平成二二年の「岡崎市立中央図書館事件（Librahack 事件）」（高木浩光「“Librahack” 事件を総括する」りぶらサポータークラブ岡崎図書館未来企画編『ネット時代の情報拠点としての図書館――“Librahack” 事件から考える――』（二〇一一年）七頁以下 <http://www.terracco.jp/etc/doc/librahack_book.pdf>）のような事象に対しても、相互理解に基づく妥当な対処のあり方の探究が重要になる。

(63) 警察庁編『平成二六年版警察白書』（二〇一四年）五一頁参照。

(64) 評釈として、帖佐隆「判批」パテント六三巻六号（二〇一〇年）二九頁、一原亜貴子「判批」岡山大学法学会雑誌六〇巻三号（二〇一一年）一一九頁がある。

(65) 只木誠「営業秘密侵害の罪」法学教室三九七号（二〇一三年）一〇〇頁参照。

(66) そのほかに、自動車販売会社の社員が本社のサーバーコンピューターにアクセスして、販促情報に関するデータファイルを私用のハードディスクにコピーした持ち出した行為に営業秘密領得罪を認めた事案（横浜簡裁平成二七年三月六日付略式命令）もある（二〇一五年三月七日付神奈川新聞報道）。

(67) 当時の議論状況について、たとえば、「特集　コンピュータ犯罪とデータの保護」刑法雑誌二八巻四号（一九八八年）に所収の各論稿を参照。

(68) たとえば、先に挙げた安富潔「情報セキュリティの刑事法的保護」法学新法一一二巻一＝二号（二〇〇五年）五八頁。なお、佐久間修「サイバー犯罪と刑法」ジュリスト一四一四号（二〇一一年）一三四頁。

(69) なお、東京地決平成一〇年二月二七日（判時一六三七号一五二頁）。同決定につき、前田雅英＝星周一郎『刑事訴訟法判例ノート〔第二版〕』（二〇一四年）八二頁、およびそこに掲記の引用の文献等参照。

(70) これに関しては多数の文献があるが、立案担当者以外のものとして、さしあたり、前田雅英「サイバー犯罪と刑事法」罪と罰四八巻四号（二〇一一年）七頁以下、池田公博「電磁的記録を含む証拠の収集・保全に向けた手続の整備」ジュリスト一四三二号（二〇一一年）七八頁。なお、平成二三年改正以前の段階での包括的な検討として、井上正仁「コンピュータ・ネットワークと証拠の収集・保全」同『強制捜査と任意捜査〔新版〕』（二〇一四年）二四〇頁（初出：法学教室二四四号・

二四五号〔二〇〇一年〕）。

（71）　警察庁『警察庁情報セキュリティ政策大系―二〇〇四』（二〇〇四年）二五頁注（35）参照〈http://www.npa.go.jp/cyber/policy/image/2004.pdf〉。

（72）　佐々木監修・前掲注（30）書五頁〔佐々木良一〕。

（73）　佐々木監修・前掲注（30）書七頁〔舟橋信〕。

（74）　羽室・前掲注（3）書三〇九頁。

（75）　島田健一「サイバー犯罪捜査とデジタルフォレンジックの実際」警察学論集六八巻三号（二〇一五年）七四頁。最高検察庁刑事部デジタルフォレンジック推進班においても、同様の定義をしているとの由である。同右八一頁注（16）。

（76）　警察庁情報技術解析課「平成二五年における情報技術解析の実施状況について（平成二六年三月一三日付公安委員会説明資料七号）」〈http://www.npsc.go.jp/report26/03-13.pdf〉。

（77）　安富潔「情報セキュリティの刑事法的保護」法学新報一一二巻一＝二号六九頁など参照。なお、ネットワーク利用形態の多様化に伴うデジタル・フォレンジックの課題を指摘するものとして、野本靖之「ネットワーク利用形態の多様化とデジタルフォレンジックの課題」警察政策一二巻（二〇一〇年）二二七頁。

（78）　同右七五頁以下。

（79）　同右七六頁以下。

（80）　拙著『防犯カメラと刑事手続』（二〇一二年）二四九頁以下。

（81）　拙稿「事前予防と秩序違反行為の法的規制」刑法雑誌五四巻三号（二〇一五年）掲載予定。

（82）　なお、井田良「社会の変化と刑法」同『変革の時代における理論刑法学』（二〇〇七年）二三頁も参照。

（83）　坂＝四方・前掲注（5）論文一七三頁以下。

（84）　拙稿・前掲注（81）論文。

（85）　先に見たように、平成二三年の刑事訴訟法一部改正では、ログの保全要請に関する規定が設けられた（一九七条三項ないし五項）。

（86）　http://www.soumu.go.jp/main_content/000254565.pdf.

（87）　林紘一郎「サイバーセキュリティと通信の秘密」土屋大洋監修『仮想戦争の終わり―サイバー戦争とセキュリティ』（二〇一四年）一八三頁以下。

（88）　従来、通信の保護対象は、「通信の内容」のみならず「通信に関わるすべての事実」、つまり「通信の存在それ自体に関す

る事柄」を包含すると解されてきた。しかし、少なくとも②認証ログについては、インターネット利用者とＩＳＰとの間で加入者であることの認証をしＩＰアドレスを割り当てるだけであって、「コミュニケーション」を行っているわけではなく、憲法二一条二項などにいう「通信」にあたるのかという疑問も生じうる。なお、ＩＣＴサービス安心・安全研究会個人情報・利用者情報等の取扱いに関するＷＧ『「電気通信事業における個人情報保護に関するガイドライン」の改正について（案）』（二〇一五年）一〇頁は、接続認証ログの保存について、「利用者の表現行為やプライバシーへの関わりは比較的小さいと考えられる」としている。いずれにせよ、「通信」の内実や、「通信の秘密」を保護する意義を、インターネットという新たな文脈において再検討する必要がある。小向太郎『情報法入門〔第二版〕』（二〇一一年）七九頁以下、石井夏生利「ＤＰＩとプライバシー・個人情報保護・通信の秘密」ＩｎｆｏＣｏｍ　ＲＥＶＩＥＷ五三号（二〇一一年）三八頁以下、高橋郁夫「インターネット媒介者の役割と『通信の秘密』」Ｎｅｘｔｃｏｍ一六号（二〇一三年）一一頁、曽我部真裕「通信の秘密の憲法解釈論」Ｎｅｘｔｃｏｍ一六号（二〇一三年）一九頁以下、石井徹哉「刑事法から見た通信の秘密」警察学論集六六巻一二号（二〇一三年）二二頁以下など。

(89)　岸田憲夫「インターネットにおける公共の秩序維持」関根謙一ほか編『講座警察法二巻』（二〇一四年）五六五頁以下。現時点でサイバーに関する捜査活動の目立った支障が顕在化していないのは、ＩＳＰが自主的に一定期間中に認証ログを保存等しているにすぎないからであるとされる。同右五六八頁。「府省庁対策基準策定のためのガイドライン（平成二六年五月一九日内閣官房情報セキュリティセンター）」基本対策事項六・一・四・(1)―三は、ログの保存期間について、標的型攻撃については、ログは一年間以上保存することが望ましいとするが、前提としてＩＳＰにおいても同程度以上の期間のログが保存されていないと、実効性に乏しい基準となる。なお、私事性的画像記録の提供等による被害の防止に関する法律（リベンジポルノ防止法）附則二条は、通信履歴等の保存のあり方について、同法施行後二年以内に検討し、必要な措置を講ずる旨を規定している。

(90)　宍戸常寿「通信の秘密について」企業と法創造九巻三号（二〇一三年）二五頁。さらに、海野敦史『「通信の秘密不可侵」の法理――ネットワーク社会における法解釈と実践』（二〇一五年）参照。

(91)　同事件で、東京地裁は、サイバー犯罪は、「インターネットの利用に関して社会に大きな不安を抱かせるとともに、コンピュータプログラムを信頼して情報処理を行うことを蹂躙させ、ひいてはインターネットやコンピュータによる情報処理の円滑な機能を阻害する重大な結果をもたらしかねないものである」などとして、被告人に対し威力業務妨害罪等で懲役八年を宣告した。東京地判平成二七年二月四日（ＬＥＸ／ＤＢ：二五五〇五九四〇）。

(92)　四方光「サイバー犯罪の特徴と諸対策遂行上の法的課題」大沢秀介編『フラット化社会における自由と安全』（二〇一四

年）一〇六頁。なお、名和利男「サイバー攻撃の主体とサイバー防御のための人材育成のあり方」土屋大洋監修『仮想戦争の終わり――サイバー戦争とセキュリティ』（二〇一四年）一〇六頁以下も参照。

(93) 平成二三年度総合セキュリティ対策会議報告書『サイバー犯罪捜査における事後追跡可能性の確保に向けた対策について』（二〇一二年）一頁以下参照。

(94) 四方光「サイバー犯罪捜査における事後追跡可能性と通信の秘密」警察学論集六六巻一二号（二〇一三年）四六頁。

(95) 岡田好史「サイバー刑法の概念と展望」専修法学論集一一八号（二〇一三年）七三頁以下参照。

(96) 佐々木監修・前掲注（30）書四七五頁〔佐々木良一〕。