サイバーセキュリティと通信の秘密に関する提言：自律システム管理責任の明確化と対象を特定した通信ログの利活用を

林紘一郎 *・田川義博 †

概要

本稿は、サイバーセキュリティ基本法に定めるサイバー関連事業者や重要社会基盤事業者（いずれも電気通信事業者を含む）に、自律システム管理責任（後者についてはその一部のみ）を課すことを明確にするとともに、責任遂行に不可欠な通信ログの利活用を正当業務行為と位置付けるため、制定法やソフト・ローの改正案を提案するものである。

第 1 部「サイバーセキュリティと『通信の秘密』」は、「通信の秘密」に関する枢要な概念と、本稿が立脚する「ログの利活用に関する 9 原則」を定義し（第 1 章）、「通信の秘密」に関する通説と対比しつつ「通信の秘密の保護とサイバーセキュリティ対策は、適正手続を守れば相補的な関係にある」とする共著者の見方を紹介し、議論の糸口とする（第 2 章）。次いで米国や EU 等の先例のうち、「自律システム管理責任」の核になる「ネットワーク・モニタリングの権限と責任」等の意義を明確にする（第 3 章）。

第2部「電気通信事業者の自律システム管理責任と通信ログの役割」は、同事業者に対象を絞った分析である。従来 hand-off を義務付けられてきたが、その修正を迫られている経緯を説明し（第 4 章）、コンテンツに関する媒介者責任である notice-and-takedown 法理とは別に、「自律システム管理責任」が必要であり、「法と経済学」の観点から裏付けられることを紹介する（第 5 章）。また、先進諸国とわが国における通信ログの利活用の現状を概観し、インテリジェンス活動における民間企業の通信ログの重要性を推定する（第 6 章）。

第 3 部「自律システム管理責任の明確化と対象を特定した通信ログの利活用」は、サイバー関連事業者・重要社会基盤事業者・電気通信事業者ごとに、法改正の具体案を提示する。まず、わが国の法制において a) モニタリング、b) そこで知得したログの自己利用、c) ログをインシデント情報に加工後の官庁等への報告、d) インシデント情報の他者との共有の各要件を明確にし、これに伴う要改善点を列挙する（第 7 章）。そして、要改善点をハード・ローとソフト・ロー、実体法と手続法別に割り付け、サイバーセキュリティ基本法・電気通信事業法等の改正案や、新たに制定すべき省令等の方向性を提示する（第8章）とともに、刑事罰の比較を例として提案自体の自己点検を試みる（第 9 章）。

* 情報セキュリティ大学院大学名誉教授

† 情報セキュリティ大学院大学セキュアシステム研究所客員研究員

第1部　サイバーセキュリティと「通信の秘密」

1　「通信の秘密」「通信ログ」などの枢要な概念

1.1 「サイバーセキュリティと通信の秘密」というアプローチ

サイバーセキュリティについて論ずる場合、マクロとミクロに分けて考えることができる。しかし、最近発覚した三菱電機の機密情報漏えい事件は [1]、一方で被害企業が「次の攻撃にどう備えるか」というミクロの問題であると同時に、防衛装備品のサプライチェーン全体のリスク管理策（延いては安全保障問題）というマクロ的問題でもある。ここでは、ミクロとマクロが分かちがたく結びついており、対策も従来の組織経営の常識である「縦割り」の枠を超えた、「分野横断的」な色彩が濃厚である。

また、サイバー空間には境目がないことを反映して、サイバーセキュリティの対象領域も拡大していくが [2]、新しい分野であるため「白地に絵を描く」ことが技術的には可能であるものの [3]、法律的な対応を考える場合には、むしろ経路依存性（先例拘束性、と言い換えても良い）こそを重視しなければならない。

このようにセキュリティ問題は、伝統的な分類では切り取れない要素を持っている。マクロの分析は常識的判断に馴染むが、技術的検討や手続き的担保というミクロ分析抜きで、マクロ政策の是非を論ずるのは「机上の空論」に終わる危険があり、その逆は「木を見て森も見ない」欠陥が生じがちである。どちらも議論が錯綜したままの状況に置かれ、新たな技術や攻撃手段が開発されると、その対応に追われて、それまでの議論が未整理のまま放置される、といった繰り返しになりやすい。

そこで私たちは、共に長年にわたって電気通信事業に携わった経験を生かし、「通信の秘密」や「ログの役割」といった概念を基軸にして、その視点からサイバーセキュリティを論ずるという、独自のアプローチを採ってきた。「通信の秘密」は、電気通信事業という業界でこそ知られているが、社会一般で広く議論されるものではない。その意味では玄人好みの、それもかなり技術に依存した概念である。

しかし、一見サイバーセキュリティとは疎遠と思われる概念が、実は以下の 4 点で「表裏一体」

---

[1] 概要については、以下を参照。https://digital.asahi.com/articles/ASN544T17N52ULZU00F.html?iref=pc_ss_date

[2] 自動運転車を含む IoT（Internet of Things）や暗号資産などがセキュリティの中心的課題になるということは、一昔前には予想さえできなかった。安全保障という概念も、エネルギー安保、食糧安保論に発展し、サイバー安保、宇宙安保の問題になり、アフターコロナ時代には医療安保がより重要かつ緊急性を持つであろう。

[3] 新技術が生命の危険さえ伴う場合には、研究開発の初期段階からセキュリティ対策を盛り込んでいる（例えば、自動運転車に関しては、技術的分析とハッキング分析は同時並行的に行われている）。電気通信のように役務そのものは古いが、その後の技術進歩が著しく、処理や伝送が光速で行われる分野においても、同様の即応体制が求められる。

といえるほど密接に関連していることを理解していただければ、本テーマがセキュリティ問題の切り口の 1 つになり得ることが、お分かりいただけるだろう。なお自律システムとログの定義に関しては、1.3 節と 1.4 節でまとめて論ずる。

① サイバーセキュリティはサイバー空間での情報処理や伝達の安全性を担保するものであるから、証拠としてログを分析することがリスクと対応策を理解するための第一歩となる。サイバー事案が過失から攻撃へと変化した現状では、サイバー対策は犯罪捜査に近似しており、証拠は決定的な意味を持つ [4]。

② サイバー空間の代表的存在であるインターネットにおいては、セキュリティの担保はそれを構成する自律システム（Autonomous System = AS）[5] の所有者（運営者を含む。本稿の全体を通じて、以下同じ）に委ねられているので、それぞれの所有者がログを分析し、「自己のシステムは自身で守る」ための対策を講じなければならない。つまり、ログの扱いが電気通信事業者のみならず、自律システム所有者すべてに共通の事象になる。

③ 同時に、サイバー攻撃が「攻撃者優位」の状況にある限り（林 [2015]）、防御側はインシデント情報等を所管官庁に報告することや、他者と共有することで対抗せざるを得ず、その際の情報はログから得られるものが大半を占める。

④ 上記の事実を法学的に再構成すれば、セキュリティという「目に見えない」対象を規律するには、実体法と同時に（あるいは、それ以上に）手続法が重要性を持つことになり、ログの扱いが技術問題を超えたものになっている [6]。

1.2 「通信の秘密」の規律範囲に関する大きな枠組み

サイバーセキュリティに関して、共著者は上記の方法論で多角的に論じてきたが、議論を深めようとすれば細部に入らざるを得なくなり、結果的に「木を見て森を見ず」という前節の弊を自ら招いたのではないかと反省している。そこでニュアンスの差には目をつぶり、「通信の秘密として、どのような情報の保護が、どのようなビジネスに期待されているのか」という原点に帰って整理し直すと、表 1. が得られる。縦軸が保護の客体で、横軸が保護の主体となる事業である。

表 1.「通信の秘密」の規律範囲 [7]

[4] 刑事法の研究者として、この点を強調する中野目 [2020]（特に注 7.）を参照。
[5] これは当然ながら、コンピュータがネットワークに接続されることを前提にしている。以下の記述においても、時として自律システムとネットワーク、更にはそれらを流通し保存されているデータそのものを一体として論ずることがあるが、それはこの 3 要素が不可分に結びついているためである。
[6] 手続法の重要性は「情報法」という法領域に共通の特性である（林 [2017a]）。
[7] 「通信の秘密」（電気通信事業法 4 条）に該当するために要件の 1 つとして、「電気通信事業者の取り扱い中に係る」という制約があるが、「他人が違法に傍受した通話録音記録を（何らかの方法で）入手して複数の関係者に聞かせた」場合であっても、この要件を満たすとの最高裁判決（最二小判 2004 年 4 月 19 日 刑集 58 巻 4 号 281 頁）があるほかは、その要件が裁判で争われたことがないので説明を省略した。ただし、後述の注 33 を参照。

保護の主体となる事業 保護の客体 (秘密の分類)	D. 電気通信事業	E. 適用除外電気通信事業
A. 通信の内容	①	②
B. 通信に関する制御用情報	③	④
B´通信に関するログ	⑤	⑥
C. 契約者(加入者)情報	⑦	⑧

ここで、保護の客体(秘密の分類)と保護の主体となる事業、A～E は、次の意味である。まず「保護の客体」とは、「通信の秘密」に該当する情報、すなわち通信の当事者が秘匿することを望む情報(秘密)をいい、その態様に従って以下の 4 者に分類される。

A.「通信の内容」は、電気通信事業法 4 条 1 項にいう「通信の秘密」の中核をなし、通話・メール・検索・ダウンロードなど、電気通信を介して知得される情報内容をいう。

B.「通信に関する制御用情報」は、電気通信の接続のために必要な情報で、電気通信の当事者・アドレスなどの識別番号のほか、その集計結果である通信回数など、通信の内容が推知される可能性があるものをいう[8]。

B´「通信に関するログ」は、上記 B および伝送途上においてシステムによって自動的に付加される信号(例えば、セッションの開始・終了時刻等)であって、通信の終了後も一定期間事業者に保存されるものをいう。

C.「契約者(加入者)情報」は、電気通信事業者が契約の履行に必要なため保有する名・住所・料金支払い方法・口座番号など利用者に関する情報をいう。

次に「保護の主体となる事業」とは、「通信の秘密」を守ることが義務付けられている事業であり、以下の 2 者に分類される。

D.「電気通信事業」とは、電気通信事業法2条四号の定義に当てはまる事業で 、規律の主たる対象である。

E.「適用除外電気通信事業」とは、同法 164 条 1 項において原則として法の適用外に置かれつつも、なお電気通信事業の性格を失わないことから、「検閲の禁止」と「通信の秘密」に関しては同条 3 項において順守義務を課せられている事業をいう[9]。これには、一号＝親会社にのみ電気通信サービスを提供する子会社、二号＝同一構内に閉じたネットワーク、三号＝「電気通信設備を用いて他人の通信を媒介する電気通信役務以外の電気通信役務(ドメイン名電気通信役務を除く。)を電気通信回線設備を設置する

[8] 共著者は、B と B´は法 4 条 2 項の「他人の秘密」に該当し、同 1 項の「通信の秘密」とは別の概念ではないかと考えてきたが(インターネットと通信の秘密研究会 [2013] など)、議論の複雑化を避けるため第 9 章でまとめて論ずる。

[9] 「電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供する」役務(事業法 2 条三号)を「他人の需要に応ずるために提供する」(同四号)者は「電気通信事業者」であるが、それらの事業者は登録あるいは届出を要する(同五号)。しかし登録や届出を欠く事業者であっても「電気通信」と同様の機能を果たすサービスを提供している者には、(事業者単位ではなく)当該サービスに限定した「通信の秘密」保護の義務が課せられる。

ことなく提供する電気通信事業」の 3 タイプが含まれるが、本稿のテーマに関係するのは、ほとんど第三のタイプである[10]。

1.3 「自律システム」の一般的定義

現在の通信ネットワークの中核をなすインターネットは、様々な管理主体が運用する通信ネットワークの相互接続で成り立っている、「ネットワークのネットワーク」である。その構成単位となり、個々の通信事業者やインターネットサービスプロバイダ（ISP＝Internet Service Provider）、ユーザ企業などが、それぞれの運用方針や制御情報に基づいて相互接続するネットワークを、自律システム（AS）という。

つまり AS とは、「インターネットを構成する単位となる、ある一つの管理主体によって保有・運用されている独立したネットワーク。単一の経路制御（ルーティング）ポリシーを共有するネットワークで、外部から一つの塊として認識される」(IT 用語辞典 e-Words)というのが、技術的には不正確かもしれないが、最も分かりやすい説明になろう。複雑で技術進歩が激しいインターネットの世界では、概念自体も変化を免れないからである。

Wikipedia によれば、AS はもともと Border Gateway Protocol (BGP) に関する RFC 1771（1995 年 3 月）において「インターネットサービスプロバイダ (ISP) や複数のネットワークに繋がった巨大な組織など、ひとつのルーティングポリシーによって制御されているネットワーク」と定義されていた。しかし RFC 1930（1996 年 3 月）では、「グローバル AS 番号を持った ISP に繋がっている複数の組織においてプライベート AS 番号を使用して BGP を走らせ、インターネットに繋ぐことができるようになった」ので、「たとえその ISP が複数の AS を抱えていても、インターネットからは ISP のルーティングポリシーが見えるだけ」となり、定義がより難しくなったとされる[11]。

AS には固有の識別番号（AS 番号）が割り当てられ、経路選択の際のネットワークの識別や指定などに用いられる。インターネット上でのパケットの経路制御（ルーティング）は AS 間と AS 内で分かれており、それぞれ異なるルーティング・プロトコル（通信規約）や経路情報が用いられる。法的な比喩で言えば、AS 内は一種の治外法権にも似て、AS 所有者の自主・自律的な管理に委ねられている。

そこで、自律システムの管理について何らかの規律を導入することは、片方で（一定の）自治自律を容認しつつ、他方で（別種の）規律の維持を要請するという難題を抱えることになる。

---

[10] 第 1 項三号の事業を「第三号事業」と呼ぶことは一般化しているが、第 1 項全体を指す「適用除外電気通信事業」は共著者が便宜上名付けたにすぎない。これらの規定は、事業法制定前の公衆電気通信法における「回線開放」の経緯を踏まえなければ理解できないので、細部は高嶋 [2015](pp. 58-63)を参照されたい。なおドメイン名電気通信役務に関しては、後述（2.1 節）の漫画村事件を参照。

[11] しかし RFC1930 においても、RFC1771 における以下の特性は、失われていないと思われる。’The use of the term Autonomous System here stresses the fact that, even when multiple IGPs（Inter Gateway Protocols）and metrics are used, the administration of an AS appears to other ASs to have a single interior routing plan and presents a consistent picture of what destinations are reachable through it.

これを完全に解消する名案はないが、制定法という「ハード・ロー」以外に、「法的な拘束力がないにもかかわらず、現実の経済社会において国や企業が何らかの拘束感をもって従っている規範」である「ソフト・ロー」[12] によって代替するか、両者の組合せを工夫するなどの方策が求められよう。

また、ここでいう「何らかの規律」は誰に宛てたものかという問題（法学では「名宛人」問題という）も生ずる。この点に関して共著者は、原則として「自律システム」には（注 5. で述べたように）「コンピュータとネットワーク、時にはそこで扱われる情報そのもの」を含むものと考え、「自律システム管理者」は「これら 3 要素の 1 つ以上の所有者または運営者」であり、その利用者は含まれないものと解している。「概念があまりに漠然としている」との批判は甘受するが、ハード・ローだけでは対応できずソフト・ローも含めた規律とならざるを得ないこと、技術の変化に依存せざるを得ないことから、さし向きのお許しを得たい。

1.4 「ログ」の一般的定義

電気通信ネットワークも AS の一種であり、これは、かつて両端の機器（端末という用語が象徴するように単機能のものであった）まで電気通信事業者の管理下にあった電話型システムとは、全く対照的である。ここではコンピュータの軽薄短小化が最大限に生かされているため、電話ネットワークのように「重たい」ものではなく、コストが安く仕様の変更が容易なので、導入が早くできるため広く普及してきた。

しかし「軽さ」を追及するために、利用者の倫理観に信頼をおいてきたため、セキュリティへの配慮は十分とは言えなかった。その脆弱性を突く形でサイバー攻撃が顕在化したため、インターネットの自律・分散・協調の良さを守ろうとするなら、自律システムの所有者に一定の責任を持ってもらうことが必須となっている。

そのような一定の責任を全うするには、コンピュータ処理に関する記録であるログが欠かせない。ログとは、「起こった出来事についての情報などを一定の形式で時系列的に記録・蓄積したデータのこと。船の航海記録（日誌）が原義」である（IT 用語辞典 eWord）。ログの種類や分類には定説はないが、総務省の「国民のための情報セキュリティサイト」では、表2. のような説明がなされている [13]。

表2.「国民のための情報セキュリティサイト」におけるログの説明 [14]

ログの具体的な例としては次のものが挙げられます。

[12] 『ソフト・ロー研究叢書』（全 3 巻、2008 年～2010 年、有斐閣）における定義。また、政府規制対自由市場という二項対立的な発想ではなく、官と民が協調して秩序を維持するという「共同規制」の発想（例えば、生貝 [2011]）も、ソフト・ローと親和性があり検討に値する。

[13] https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/22.html

[14] 表 2. における 12 個のログの例示はランダムに並んでいるように見えるが、上から 3 つが後述の「通信ログ」で、次の 8 つが情報処理に関するログ、最後の 1 つは異質なログ、と分けられそうである。しかし web メール（や web 会議システム）のように、メール的（ビデオ会議システム的）要素と web 的要素が不可分の場合には、区分に無理が生ずる。

・ファイアーウォールを通過した通信、または拒否された通信のログ
・侵入検知システム（IDS）や侵入防止システム（IPS）が監視した通信のログ
・DHCP サーバがパソコンに IP アドレスを割り当てたログ
・ファイルサーバへのアクセスのログ
・ファイルの参照や、編集などの成功や失敗のログ
・情報システムへのログイン、ログアウトなど認証の成功や失敗のログ
・Web サーバへのアクセスのログ
・Web サーバが利用者から受け取った入力内容のログ
・Web プロキシサーバが中継した通信のログ
・データベースサーバへのアクセスのログ
・アプリケーションが出力する処理結果の正常終了、異常終了などのログ
・パソコンの監査のログ

それぞれのサーバやシステムが出力するログの内容は、通信やアクセスの送信元・送信先の IP アドレスを始めとして、通信に使用されるポート番号、命令の内容、通信データ自身など、さまざまなレベルがあります。出力されるログの詳細度は一般的には設定によって制御できますが、どのような内容のログを取得するべきかは、組織が扱うデータの性質や、システムの処理能力、ネットワーク構成などに大きく関係します。
さらに、組織が受ける可能性があるネットワーク攻撃を事前に想定し、それを考慮したログの取得・管理方法を設計に反映することで、調査が必要になった場合に、より役に立つ情報を得られることが考えられます。
必要なログの種類と内容について、組織内で十分に検討を行い、適切なログを取得できるようにしましょう。

このように広義のログは、AS から出力される、あらゆる処理記録を指すものであるが、その広汎性故に、窃用や漏えいによりプライバシー侵害が生じた場合、被害が甚大になる恐れがある。プロファイリングにつながる情報を多数含んでいるからである。そこで私たちの検討がプライバシーへの配慮を欠くことがないよう、ログの取り扱いに関する 9 原則を、表3. のようにあらかじめ定めておきたい。

表 3. 自律システムの所有者（運営者を含む）によるログの利活用に関する 9 原則

① 目的：サイバーセキュリティ対策に生かす場合に限る、
② バルク知得と速やかな特定データへの変換：バルクデータとして一旦知得することはできるが、精査を要する情報だけを特定した上で他は速やかに消去しなければならない、
③ 自己利用の自由：特定データは自己利用することができる、
④ 報告の奨励：精査を要する特定データを匿名化してインシデント情報に加工し、所管官庁等へ報告することが奨励され、

⑤ 共有の許容：インシデント情報を他者と共有することができるが、
⑥ 匿名性の維持：捜索差押令状などの正規の要請がない限り個人識別データと突合せず、
⑦ 消去：一定期間が経過すれば復元困難な形で消去しなければならず、
⑧ 情報保全：全プロセスを通じて情報の保全に責任を負い、
⑨ 監査：全プロセスが正しく実行されているか第三者による定期的なチェックを受ける。

上記の 9 原則は、共著者のアイディアから出たものであるが、総務省と国立研究開発法人情報通信研究機構（NICT＝National Institute of Information and Communications Technology）が ISP と連携して実施している IoT 機器の脆弱性探知と通知活動である NOTICE（National Operation Towards IoT Clean Environment）における、プライバシーへの慎重な配慮を参考にしたものでもある[15]。

というのも、NOTICE は「IoT 機器に設定されているパスワードが容易に推測されるもの（「password」や「123456」など）かどうかを確認するもの」（NICT のプレス・リリース[16]）に過ぎないため、本稿で提言する「ログの知得」すら行っていない。しかし、その実施計画は総務大臣の認可を要し、厳格な安全管理措置を伴うものである。これは「通信の秘密」の所管官庁が自ら参画するという事情もあろうが、学ぶべき点があると考えた。

なお、本稿で検討の対象とするログは、「ログ」全般を指す場合と、「通信ログ」に限定する場合の両方がある。表3. はいずれのログにも適用されるが、法的な検討が必要なのはほとんど後者に限られる。そこで、「通信の秘密」の保護下にあるログの扱いを論ずる場合に、誤解を避けるため「通信ログ」と表記することがあるが、その場合「通信ログ」以外のログは原則的に利活用が自由であることを、忘れないでいただきたい[17]。

ところで、このような説明に対して読者の多くは「分かったようで分からない」というモヤモヤ感から逃れられないのではないか、と推測する。というのも、ログの細かい定義や分類は AS 毎に自由で、標準化もなされていないため[18]、AS に依存しない説明ができないからである。そこで、法的な比喩（metaphor）にはリスクが伴うことを覚悟のうえで[19]、「semantic 的利用」と「syntactic 的利用」という区分を用いることをお許しいただきたい。

前者は情報が持つ意味を利用し、後者は意味を捨象したシャノン的利用しかしないものである。前者の代表例は通話の内容・メールの内容・検索結果の内容などであり、それ自体がプライバシー情報と思われるものである。他方、後者の代表例は発信 ID・受信 ID・セッション開始時刻・サイトへのアクセス情報等であり、それらを大量に収集し分析すればプライバシー情報

[15] 同活動は「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が、2018 年 11 月 1 日に施行されて可能になった。
[16] https://www.nict.go.jp/press/2020/05/15-1.html
[17] といっても、プライバシーや個人データ保護の責任を免除するものではないのは当然であり、その限りで「ログの利活用に関する 9 原則」は、ソフト・ローとして機能することが期待される。
[18] IBM がログの標準化の案を示し、業界団体の OASIS（Organization for Advancement of Structured Information Standards）の部会で 2005 年に採択されたが、普及していない。
[19] 田村［2020］は、著作権法解釈における metaphor 依存の危険を指摘している。

に近付くが、「名寄せ」などの行為を行わない限り、プライシーの侵害になるとは言えないものである。表1. に掲げた「A. 通信の内容」が前者で、「B´通信に関するログ」が後者に当たることは、容易にお分かりかと思う[20]。

この分類によれば「通信ログ」の利活用は「syntactic 的利用」に該当し、個人情報保護法の理念と手続を守れば、それ自身によるプライバシー侵害の度合いは相対的に軽微であり、使い方次第で善用も悪用もできる。上述した「ログの利活用に関する 9 原則」は、「ログは悪用しないし、合法的な利活用の際も、プライバシー侵害のリスクを最小化する努力を惜しまない」という宣言であり、その限りで利活用が認められるべきだと思われる[21]。

1.5 ログの扱いにおける「通信屋」と「コンピュータ屋」の違い

ところで、コンピュータと通信ネットワークは別々に発展してきたので、それぞれの技術者が自身の担当する業務に誇りと愛着を持てば持つほど、「通信屋」と「コンピュータ屋」という別々のメンタリティが生ずることになり、現在でも名残が残っている。更に悪いことに、わが国では「通信の秘密」が厳格に解釈・運用されてきたため、その理解が深い「通信屋」と、自由市場でその点への配慮の度合いが低かった「コンピュータ屋」のメンタル面での分断を、助長してきた経緯もある 。

以上の状況を、やや戯画化して表にすれば、表 4. のようになろう。なお、この対比は万国共通ではなく、「通信の秘密」が厳格に解釈・運用されてきた、「（わが国の）通信屋」に固有の現象かもしれないが、次のエピソードは笑いごとで済ますことができないことを暗示している。

共著者の 1 人の林は、デジタル・フォレンジック研究会の創設以来の会員であるが、同研究会編の『デジタル・フォレンジック事典』に「フォレンジックと通信の秘密」に関する記述がみられないことを残念に思っていた。そこで改訂版が出版されるのを機に、自ら志願して 1 節を新設・執筆する提案を了承してもらった。しかし、そこで発見した意外な事実は、フォレンジックのプロである会員の間でさえ、「通信の秘密」に該当する情報の扱いに特別の配慮（個人情報への配慮とも違った配慮）が必要であることを理解している人は、ごく限られていたことである[22]。

表 4.「通信屋」と「コンピュータ屋」の理解

項目	（わが国の）通信屋	コンピュータ屋
政府規制一般	電気通信事業は、かつては殆どの	コンピュータ産業は「言論の自由」の

[20] 米国の ECPA（Electronic Communications Privacy Act of 1986）では、前者を第 1 編の Wiretap Act で、後者を第 2 編の Stored Communications Act で律するなど、両者を明確に区分している。

[21] 3.4 節で紹介予定の、仏国 2016 年デジタル共和国法における郵便・電子通信法典の改正による、「通信の秘密は、通信の内容、通信当事者の身元（identité）、メッセージの表題及び通信に添付された文書に及ぶ」とする規定は前者を想定したものである。また、わが国の著作権法における「著作物に表現された思想又は感情の享受」（同法 2 条 1 項一号、同 17 条）と「それを目的としない利用」（同 30 条の 4）は正に両者の区分に相当するものである（福岡・松村 [2019]）。

[22] これは、『改訂版デジタル・フォレンジック事典』（2014 年）の執筆当時のことであり、現在では払拭されているものと期待している。

	国で官営だったし、民営化しても公益性を有するので、政府規制があるのは当然である	一翼を担っているので、政府規制を受けたことがないし、受けるべき理由がない
電気通信事業法の適用	事業を行う上で守らねばならぬ基本法である	原則として適用されない
ログの扱い	「通信の秘密の一部」であり、その利活用は原則として禁じられていると解されている	「通信の秘密」とは別に、プライバシーの観点から保護されるが、利用者の同意を得て、情報保全義務を満たしつつ、自由に利活用している

いずれにせよ、インターネットが基幹ネットワークになった現代においては、このような争いは「内輪揉め」に過ぎないから、早期に脱却すべきであろう。その際妥当な方法は、2.2 節を先取りしていえば、過剰とされる「通信の秘密」の内容をアンバンドルして、利活用を認める部分を明確にする一方、過少とされる適用除外電気通信事業にも（アンバンドル後の）「通信の秘密」の規定を電気通信事業者と同じレベルで適用すること、つまりは両者のイコール・フッティングを図ることであろう。

誤解を恐れずに言えば、「通信の秘密」に濃淡を認め、少なくともログに関しては広く（対象事業の範囲を広め）、薄く（サイバー対策としての利活用が正当業務行為であることを認めつつ）適用することが妥当かと思われる。

2 「通信の秘密」の解釈と本稿の出発点

2.1 従来の通説と未検討部分

さて、概念の説明はこの辺りで止め、前出の表 1. に戻ろう。この表の解釈に関するわが国の通説は、保護の客体から契約者情報（C）を除いた部分[23]、すなわち ①～⑥（表における網掛け部分）が「通信の秘密」の規律対象であり、その要素の間に表 1. の縦軸のような差はないと解している。これは保護の客体である「通信」の分類に関して、C は範囲外として、残りの A・B・B´の 3 者は一体である（つまりバンドルされているし、されるべきである）との理解である。

これに対して共著者の考え方は、網掛け部分を規律の対象にすることに異論はないが、（A）と（B+B´）をアンバンドルする（これが表 1. の意味である）とともに、従来明確にされなかった ⑤ ⑥ を共に「通信ログ」と認識し、その意義を明確にしようとするものである。通信ログ B´は、

[23] 「通信の秘密」の概念から除かれるというだけで、別途個人情報保護法違反やプライバシー侵害として救済されることは、当然あり得る。

リアルタイムで行われた B に関する処理結果を、履歴として電磁的に記録するとともに、それ以外の付帯的情報も記録するため、B と完全に一致するものではないと同時に、先進諸国のおいては「通信の内容」である A とは別の扱いを受けるのが通例だからである[24]。

わが国の通説の考え方は、電気通信事業法の前身である公衆電気通信法（1953 年法律第 97 号）の時代に生まれ[25]、電気通信が独占事業であった時代の解釈を経て、通信自由化後の現行法（1984 年法律第 84 号）の解釈にも引き継がれている[26]。しかし こうした解釈は電話が中心の時代になされたものなので、以下のような未検討部分を残していた。

a) 当時の交換方式は straight-forward で、通信の記録を残さないものだったため[27]、③ と ④ の対が通信時に利用される制御用情報のすべてで、それが事後的に記録された ⑤ と ⑥ 、すなわち本稿の主題の 1 つである通信ログは事実上存在せず、議論もされなかった[28]。
b) E. の適用除外電気通信事業の概念も、後述の VAN 論争等を経て電気通信事業法の制定時に初めて生まれたもので、それ以前（つまり 1952 年から 1984 年まで）には議論の対象にならなかった。
c) 通信は電気通信事業者の媒介により成り立つが、どこまでが利用者の「通信」行為で、どこからが「媒介」行為であるかが、インターネットの登場で不分明になった。

上記の諸点は、事業法制定後 30 年以上も顕在化することはなかったが、c) に関する部分が、2017 年から 18 年初頭にかけて世間を騒がせた、いわゆる「漫画村事件」という意外なところで問題化した[29]。ここで、著作権侵害情報に対する「通信の遮断」（サイトブロッキング）が「通信の秘密」侵害行為であるかが主要な論点になり、その手段の 1 つである DNS ブロッキング[30]は、そもそも「通信の秘密」が合理的に期待される「通信」であるか否かが、初めて本格的に議論されるところとなった。

大方の論者は「通信の秘密」の伝統的解釈に基づき、DNS への問い合わせ（名前解決という）は「通信」に該当するとして侵害を肯定しているが、厳密に検討すれば「通信」ではないとす

---

[24] B は B´の部分集合であるため、以下の論議では A と B´のアンバンドルという形で論ずることが多い。これに対して従来の通説は、電話交換を前提にしていたため、以下の注 25 および 26 のような議論を当然のこととしていた。

[25] 公衆電気通信法の制定に携わった共著者による金光・吉田 [1953] は、「『通信の秘密』とは、通信の内容は勿論、誰から誰への通信であるかと云う事実又は場合により単に通信の存在の事実をも意味し、（以下略）」と説いていた。「通信の秘密」が「通信の構成要素全般や、通信の存在の有無まで含まれる」と解されるようになったのは、この解釈に源流がある。

[26] 電気通信法コンメンタール編集委員会 [1973] は、「『通信の秘密』として保護される対象には、通信の内容はもちろん、通信の当事者（発信人、受信人の居所、氏名）、発信地・受信地、通信回数、通信年月日など通信の意味内容となるものではないが、通信そのものの構成要素であり、これらの事項を知られることによって通信の意味内容が推知されるような事項は、すべて含まれる」と説いていた。現行法の解説書である多賀谷ほか [2008] も、この解釈をほぼそのまま踏襲している。

[27] 現在の交換方式は、コンピュータ・システムと同じ store-and-forward であり、運ばれる情報が一旦システムに蓄積された後で再送出され、同時にバック・アップ等のためログが一定期間保管される。

[28] Straight-forward 方式であった米国では万を超える電話会社が存在し、その間で料金の精算をする必要があったため、料金明細システムとしてログ情報が使用されていた。わが国も 1960 年代中葉に、この方式を検討したが経済的に見合わないとの判断から中断し、実用化されたのは 1970 年代末であった。このような歴史の差が、ログの扱いに関する国民の感覚に影響しているかもしれない。

[29] 海賊版の漫画ビューアサイトである「漫画村」が多くのアクセスを得たのに対して、著作権者等がサイトの閉鎖やダウンロードの違法化を主張した事件。より詳しくは、林 [2020b] と同号所収の関連論文、および「漫画村事件に見るインターネットの曲がり角」『情報法のリーガル・マインド その日 その日（第 50 回）』を参照。 http://www.cyberliteracy.com/cll/category/k_hayashi

[30] ユーザが Domain Name System（DNS）サーバへ Uniform Resource Locator（URL）を送信して通信先の IP アドレスを問い合わせる際に、問い合わせに応答させない、または警告ページへの転送を行うことによりブロックする方式。

るユニークだが有力な見方がある（伊藤・前田 [2017]）。同論文によれば名前解決は、かつて手動交換手が電話番号を調べていたようなもので事業者の内部処理プロセスにほかならず、そもそも法が想定する「通信」には当たらないと解するものである。

しかし、この解釈は DNS ブロッキングにおける通信が、「電気通信役務」の定義のうち「他人の通信の媒介」（電気通信事業法 2 条三号前段）には当たらないというだけで、「電気通信設備を他人の通信の用に供する」（同条同号後段）に当たるかどうかを検討していない（林 [2020a]）。実は DNS サービスはインターネットで通信を行う際に不可欠であり、その信頼性を担保する必要から 2015 年の電気通信事業法の改正により、「他人の通信を媒介する電気通信役務以外の電気通信役務」として適用除外とされていたものを「ドメイン名電気通信役務」という概念で新たに同法の適用対象とした経緯があるから [31]、伊藤・前田説を採ることは難しいだろう。

むしろ本件は、「通信の秘密」侵害よりも、「検閲の禁止」（事業法 3 条、憲法 21 条 2 項前段）や「利用の公平」の侵害（事業法 6 条）につながる恐れがあると考えるべきで、その懸念が広がったからこそ、大きな問題になったと思われる。

両者はともに、国家権力に対するものだと考えられてきたが、今日では「私企業による検閲・差別類似行為」（特にプラットフォーマーと呼ばれるグローバル企業によるプライバシー侵害）に、より強い懸念が示されている。また、いわゆる「違法・有害情報対策」は、媒介者である電気通信事業者の協力（つまり「利用の公平」の侵害）なくして、実効性を確保できないからである。

いずれにせよ、従来「通信の秘密」と「検閲の禁止」の関係について、憲法学者が大いに議論してきたという歴史はないようである。それだけ侵害が少なかったとすれば、その事実自体は大いに評価されるべきことであるが、漫画村事件を機に「言論の自由」と「検閲の禁止」の面から議論する憲法学者が増えたのは [32]、喜ばしいことである。

2.2 通説における「保護の過剰」と「保護の過少」

通説に基づく解釈と運用は、インターネットが基幹通信網となった現時点では、一方で「保護が過剰」であり他方で「保護が過少」であるとの懸念を生んでいる（この点を早くから指摘していたものとして、田川 [2013]）[33]。

「保護が過剰」とは、表 1. における ①～⑥ を一括して（厳密な）保護対象とすることから生ずる問題で [34]、「通信の秘密」の保護に傾きすぎ、合法的な範囲での通信ログの利活用が軽

[31] https://www.soumu.go.jp/menu_seisaku/ictseisaku/domain/index.html
[32] 宍戸常寿「ブロッキングの法制度整備に関する憲法上の論点の検討」「第 4 回インターネットの海賊版対策に関する検討会議議事録」、成原 [2018a] など。
[33] 注 7 で述べた「電気通信事業者の取扱中に係る」という要件は、GPS などの位置情報について 2013 年以降問題となり、同じ位置情報でも「取扱中」に取得されたものは通信の秘密に該当する一方で、そうでないものは、プライバシー性が高い場合であっても、通信の秘密には該当しないと整理されている。これも「保護の過少」の一例かとも考えられるので、今後も注視していきたい。
[34] 前述の注 25 および 26 によれば、①～⑧ のすべてが「通信の秘密」として保護されるかのようであるが、個人データ保護の議

視されがちなことである。後述（6.1 節）するように、先進諸国においては「通信の内容」と「通信ログ」の扱いが別建てになっており [35]、後者をサイバー対策に最大限活用しているが、わが国では利活用が著しく制限される結果となっている。

それと裏腹に、「保護が過少」の弊害は 2 点ある。まず「通信の秘密」が憲法に基礎を置くとはいえ [36]、その具体的運用は電気通信事業で顕在化することがほとんどであるため、事業者規制に重きがおかれて、電気通信事業者でない者への適用は稀であった（つまり、D のみに適用され、E に適用されることはほぼなかった）ことである。しかし最近は、GAFA（Google、Amazon、Facebook、Apple）のような巨大 OTT（Over-The-Top）企業におけるプライバシー侵害が国際問題となったため、 電気通信事業法が改正されたので、この過少は改善に向かうことが期待される [37] [38]。

もう 1 つの、より深刻な過少は、⑤ と ⑥ における「通信ログの利活用」の面で顕在化しており、ここには電気通信と非電気通信という 2 分法が影響を与えている。これはメディア規制のあり方に関する PBC 分類（4.2 で後述する）にも関連するが、より直接的には「電気通信事業に対する規律をコンピュータ通信にも適用すべきか」という議論の結果であったともいえる。というのも、日米ともに「電気通信事業者にはコモン・キャリアとして hands-off の義務があり [39]、コンピュータ通信事業者には何らの規制もない」という理解が一般化しているからである。

この問題に関する議論は、いわゆる VAN 論争 [40] として 1970 年代末から 80 年代前半にかけて、わが国でも大いに盛り上がりを見せた。しかし、わが国では米国のように「電気通信とコンピュータ通信を峻別する」という法制を採らなかったため、事業者や官庁間のヘゲモニー争いよりも [41]、専用線と公衆網の接続などにより利用者の便益を向上させることの是非論として論じられた趣があった [42]。

論の高まりとともに、今日では C は除くとする見方が通説化している。

[35] 電気通信ビジネスにおけるログは、わが国では「通信の内容ではないがその構成要素」であるとされるが、先進諸国においては「通信の内容」の保護とは切り離して扱われ（メタデータ、トラフィック・データなど様々な呼称で呼ばれ）、わが国の通説のようなバンドルした扱いは受けていない。米国では、注 20 で述べたように、根拠法である ECPA において、Interception と Stored Communications の利活用は明確に区別され、ログは契約者情報等とともに後者に属する。また通信の接続のためにプロバイダに提供する情報には「プライバシーの合理的期待」が及ばないとする Third Party Doctrine が判例で認められている。

[36] 憲法上の「通信の秘密」は、「通信の秘密は、これを侵してはならない」（21 条 2 項後段）のほか、言論の自由が根拠だとすれば「集会、結社及び言論、出版その他一切の表現の自由」（21 条 1 項）、プライバシーが根拠だとすれば「自由及び幸福追求に対する国民の権利」（13 条）、「侵入、捜索及び押収を受けることのない権利」（35 条 1 項）などにより複合的に保障されている（井上[1997]）。

[37] 「外国法人等は、電気通信事業を営もうとする場合には、国内における代表者又は国内における代理人を定めなければならないこととすること。」などの改正が行われた（2020 年 5 月 15 日成立）。https://www.soumu.go.jp/main_content/000687566.pdf

[38] ただし GAFA が適用を免れていたのは、「電気通信事業を営んでいる外国法人である」ことと、「役務の中核が電気通信ではなく情報処理である」ことが重層的に作用し、規制当局の関与を躊躇させたことにあるかと思われるので、後者の過少は依然として残るかもしれない。

[39] 「コモン・キャリアは運ばれる客体に関与してはならず、顧客を差別することなく客体を運ばねばならない」という義務。運輸・エネルギーなどのコモン・キャリアにも適用されるが、通信キャリアに最も端的に現れる（林 [1989]）。

[40] VAN とは Value-Added Network の略で、ネットワーク側にインテリジェンスを持たせ、プロトコルの違うコンピュータの相互通信を実現すればビジネス・チャンスになると考えられたため、産業界の関心を呼んだ概念である。インターネットが実現した今日では、エンド（エッジ）側にインテリジェンスを持たせるのが主流なので（Saltzer, Reed and Clark [1984]）、それに反するアーキテクチャということになる。

[41] 通信寄りの者は「データ通信」と、情報処理寄りの者は「オンライン情報処理」と呼んだ。

[42] 最も激しい議論になったのが「公―専―公」接続問題であった。専用線（固定料金で割安）を間にして、両端を公衆網（従量制で割高）でつなげば、全体としての利用料金を大幅に安くすることができるが、このような利用法を認めるか否かで、電気通信事業者と利用者の間に激しい議論があった。

ところが海の向こうの米国では、電話事業は創業以来民営で行われ、次第に「公益事業規制」（参入・撤退や料金規制）に服するようになったが（林・田川［1994］）、コンピュータ産業は製造業としてもサービス業としても一度も政府規制を受けないまま発展してきた。そこへ「コンピュータ通信」という新しいビジネス領域が誕生して両者が融合し、成長産業になる予兆があったので、これが 1934 年通信法（これは現行法でもある）第 2 編（Title Ⅱ）の「コモン・キャリア」としての適用を受けるかどうかが争われた（林［1998a］）。

当時はコンピュータ業界のロビーイング力が強く、1996 年の通信法改正に当たって、従来の「基本サービス」(Basic Service)のほかに「高度サービス」（Enhanced Service）のカテゴリーが新設され [43]、後者は通信法の適用を免れることになった。またインターネットを国策として推進し、産業競争力を強化としようとするクリントン・ゴア政権の意向で、「インターネット非規制政策」が採られたので、コンピュータ業界にはいかなる政府規制も及ばないかに見えた（林［2002］）。

こうした「インターネット自由経済圏」の扱いは、GAFA に代表される IT 産業の成功を導く素地を作ったかのように思われたが、彼らの市場支配力が誰の目にも明らかになると、それに対する反作用も見られるようになった [44]。時の政権も、シリコンバレーを応援すべきか（その場合非規制を継続することになる）、利用者側に立つべきか（何らかの規制を課すことになる）逡巡するため、政策の方向性が不明確なままであり、これに米国に特有の裁判リスクが加わり、コンピュータ通信の扱いは今後の問題として残されている。

2.3 林・田川 [2019] の踏襲と新しい視点

さて、このような通説的理解に対して、私たちは林・田川［2019］において、「通信の秘密」に関して以下の 6 点の分節化（アンバンドル）を提案した。

① 「検閲の禁止」と「通信の秘密」を区分し、
② 「通信の内容」に触れる場合と「ログ」に触れる場合を切り分け、
③ 違法・有害情報に対処するケースと [45]、インターネット・サービスの安定的提供を確保するためのサイバーセキュリティ対策を場合分けし、
④ 違法性阻却事由としての「利用者の同意」も前項の分類に合わせて再考し、
⑤ 従来「知得・窃用・漏示」として一括して議論してきたものを要素ごとに分解し、
⑥ 知得する範囲を限定した「特定データ」と、それを指定しないで悉皆的に知得する

[43] より厳密にいえば、1980 年の第 2 次コンピュータ調査（調査という名称であるが、一種の行政決定を含む）で「基本通信サービス」と「高度通信サービス」の区分が導入され、1996 年電気通信法で「基本サービス」「高度サービス」に修正された。
[44] 最近では、SNS の提供者が、1998 年通信品位法 230 条（その後 47 U.S.C. 230 となる）の免責の適用を受ける distributor に過ぎないのか、編集権を持ちコンテンツに責任を負う publisher なのかが、激しい議論を呼んでいる。争いになる条文は次の通り。47 U.S.C. 230 – Protection for private blocking and screening of offensive material (c) Protection for “Good Samaritan” blocking and screening of offensive material (1) Treatment of publisher or speaker ‘No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.’
[45] 違法情報と有害情報に関する対応は当然異なるが、ここでは一般的な用語として両者を一括している。また有害情報か否かの判断は慎重を要するので「いわゆる有害情報」という限定を付してきたが、これまた一般的な用法に従って、しばしば省略する。

「バルクデータ」の扱いを別にする。

そして、① を与件とし、② に関してはログに特化し、③ サイバーセキュリティ対策としてのログの知得・利用を、いわゆる「違法・有害情報」に対する「違法性阻却」とは「別建て」とする案を検討した。併せて ④ ⑤ においては、「ログの 知得・利用・廃棄」の正当な手続きと，濫用を防止する制度的な仕組み（情報保全のあり方）を探った。その中心的論点は、ログのライフ・サイクルに合わせた、正当な知得、目的内利用、安全管理および保存期間のルール化といった、適正運用をどのように担保するかであった[46]。

本稿は、このうち ② を前提に ③ ④ に関して更に議論を深め、「インターネット・サービスの安定的提供を確保するためのサイバーセキュリティ対策」としてのログの利活用（知得・利用）に関する合法的手続き（チェック機能を含む）に関して、法改正も含めた具体案を提示するものである。

なぜなら、サイバーセキュリティ対策を、いわゆる違法・有害情報対策と場合分けすることは、現時点で最も喫緊で身近なテーマであり、また林・田川［2019］に対する読者の反応から見ても、最も関心を引き付けたものだったからである。従って次節以降の検討は、上記論文で述べた考えを「基本的視点」として、それを具体化するものといえるので、表5. において、その点を再確認しておこう。

表 5. 本稿の基本的視点（林・田川［2019］、p. 16 を微修正）

違法・有害情報等の対策とインターネット・サービスの安定的提供という 2 つの要請は、「通信の秘密」の保護を制約することになる点では共通項を持っているが、その方向性は全く逆とも言える。前者においては「通信の秘密」の保護法益とプライバシーや表現の自由など他の保護法益との比較衡量を行い、どちらの法益を優先すべきかが判断される。一方後者においては、サイバーセキュリティ対策を強化するために「通信の秘密」の保護を制約することが、通信の自由など「通信の秘密」の保護法益を守ることにもなっていて、「通信の秘密」の保護とサイバーセキュリティ対策は、適正手続を守れば相補的な関係にあると考えられる。

私たちは 2013 年の共同研究以降、上記の分析を含め多くの論稿を生み出してきた。この過程で私たち自身も含め一般の認識が深まったことは間違いないが、著者としての能力不足もあり「これが最終提案だ」という具体的な改善策は提示できないでいた。そこで、この辺りで「不完全な 60 点」でも良いから、現状を改善できる具体的提案をしたいと考えるようになった。

本稿は、そのような願望を込めた提案を中心に、私たちのこれまでの研究の総括を試みるものである。その際、わが国のサイバーセキュリティに関する体制の成熟度に応じた対応を検討するとともに、先行事例として米国の 2015 年サイバーセキュリティ情報共有法や EU の NIS 指令等に学びつつ提案したい。前者は次節で検討し、後者は新しい視座を含んでいるので、次

[46] 前述の表 3.（9 原則）は、この経験を踏まえたものである。

章でまとめて論じよう。

実は「通信の秘密」は奥深い概念であり、上記以外にも論ずべき点は多い。しかし紙幅の制約に加え、提言を中心にした本稿の性質に鑑みて、できるだけ焦点を絞ることにした。そのため、既に他の論文で言及済みの諸点は、極力省略するか簡素化したことをお含みおきいただきたい[47]。

2.4 わが国のサイバーセキュリティ体制の成熟度に応じた対応

一般論として、特定の施策が有効であるためには、施策を取り巻く環境や実施者の実力とマッチしている必要がある。サイバーセキュリティのような新規の事例については、この原則は伝統的な事例にも増して重要であり、特に技術力が伴わない施策をやみくもに実施することは「百害あって一利なし」になりかねない。

現に米国では防衛装備品の調達において、請負人との間で「管理された非格付け情報（Controlled Unclassified Information = CUI）」を共有することから、国家標準技術研究所（NIST）が定めた手順を守るよう義務付けていたが、「順守を自己宣言すればよい」「受注時に順守されていなくても対応計画を提出すればよい」などの甘い運用の結果、より厳しい手順へと転換せざるを得なかった、とされる（永野 [2020]）。

私たちはこのような動向に薄々気づいていたので、林・田川 [2019] においては、サイバーセキュリティ対策の中心的機能である「インシデント情報の共有」を表 6. のように 6 段階に分けた上で、わが国は第 5 段階にあるものとして、第 6 段階に適した施策は敢えて「将来の課題」としていた。

具体的には、上記分節化の ⑥ において、ログの知得・利用はさし向き特定データ（知得する対象を予め指定する）に限り、バルクデータの知得（対象を指定しないで悉皆的に知得する）は、第 6 段階である情報収集体制を「政府対応力を強化した官民一体型」にレベル・アップする際に、再度検討することとしていたのである。

表 6. ログの利活用の 6 段階（林・田川 [2019]、p. 23 を表にしたもの）

段階	概要
第 1 段階:1 対 1 型	企業などの利用者のログ情報を、セキュリティ・ベンダ等が知得・利用するケース
第 2 段階:1 対 N 型	複数の企業などの利用者のログ情報を，セキュリティ・ベンダ等が知得・利用するケース。AI 等を利用してビックデータ・ログを知得・利用する場合がある
第 3 段階:民間共有型	JPCIRT/CC（Japan Computer Emergency Response Team

[47] なお長期間にわたって同じテーマを論じているので、私たちの考えも少しずつ変化している場合がある。[引用文献] に掲げた諸論文についても同じことが言えるので、その場合は後作が前作を修正しているものと、お考えいただきたい。

	Coordination Center) のようなセキュリティ・ベンダではない民間組織が, 会員企業からのインシデント情報を共有し, サイバーセキュリティ対策を行うケース
第 4 段階:官民協調型	IPA (Information Promotion Agency) や JC3 (Japan Cybercrime Control Center)のような政府とのつながりが強い組織が、政府部門からの委託を受けて、民間企業とインシデント情報を共有して、サイバーセキュリティ対策を行うケース:政府の間接関与
第 5 段階:官民一体型	政府組織が民間企業(ユーザ企業)とセキュリティ・ベンダ等と民間企業のインシデント情報を共有して、サイバーセキュリティ対策を行うケース:政府の直接関与
第 6 段階:政府対応力を強化した官民一体型(将来形)	政府部門でも、犯罪捜査や国家安全保障の担当官庁も参加して、サイバーセキュリティ対策(防御力強化と抑止力強化)を行うケース

しかしサイバーセキュリティ対策では、ビッグデータ(すなわちバルクデータ)でないと有効性が著しく減退するので、本稿では知得と利用をアンバンドルして、特定データを識別する前段階でのバルク知得を認め、その中から更に分析すべき対象を特定後、無関係なデータは直ちに廃棄するとともに個人を特定できないように加工し、特定データだけを利活用するという意味で、前稿の立場を部分的に修正することとしたい。

1.3 節の表 3. における「ログの利活用に関する 9 原則」は、この点を先取りしていることにお気づきの読者には、この修正を受け入れていただけるかと思う。

3 2015 年サイバーセキュリティ情報共有法等に学ぶ

3.1 Cybersecurity Information Sharing Act of 2015

セキュリティ対策としての情報共有を第 5 段階に止めることは、わが国が世界のトップ・レベルにあるとは言い難いことを認めることでもあるので、今後の改善策について先進諸国から学ぶ余地がある。

その代表格である米国は、2016 年統合予算法の一部(Division N)として「2015 年サイバーセキュリティ法」を制定した。近年議会に数多く提案されたサイバー関連の法案がやっと日の目を見たもので 5 部から構成され、その最初の部分(Title Ⅰ)である「2015 年サイバーセキュリティ情報共有法」(Cybersecurity Information Sharing Act of 2015、以下 CISA という)が、

Division N の最重要部分と考えられている（永野 [2016]）。

米国では従来から、インシデント情報を共有しようにも、① 民間が政府と共有したデータが情報公開法によって開示されるのではないか、② 共有データに含まれる個人データのプライバシーに責任を負い切れない、③ 競合会社と情報を共有することが独禁法違反とされる可能性がある、④ 提供情報により違法行為が指摘されるリスクがある、といった懸念があって、共有が期待通りに進まなかったといわれる。

この法律は、上記の 4 点の懸念を払拭するため、独禁法上等の免責に加えて、民間企業が情報ネットワーク・システムを (a) モニタリングし、(b) DM（Defensive Measures）を取ることや[48]、(c) 政府と DM や CTI（Cyber Threat Indicator）に関する情報を共有することで[49]、裁判で訴追されることはないことを保障している。a) と b) はアウトソースすることができ、書面による同意があれば、外注された企業が代わって実行できる。

そして、これらの免責規定を民間から政府へ情報が提供されるインセンティブとするほか、政府側も機密指定の情報をセキュリティ・クリアランスなど万全の情報保全と個人識別データの削除を条件に、民間に提供するなど互恵的な仕組みを作っている（林 [2017b]）。表 4. にある第 6 段階に達している国の代表は米国であり、インテリジェンス機関を含めた政府機関には膨大なサイバー関連情報が蓄積されているので、この互恵システムは強力である。

(a)モニタリング、(b) DM の共有と実施、(c) CTI の共有は別々の概念であり、IoT システムの場合のように、(b) の実施が自動化されているケースもあるかもしれない。しかし一般的な業務システムでは (a) が出発点であり、これ無くして次の 2 つはあり得ない。CISA での monitor の概念は、“to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system;” と技術的な側面から定義されているが[50]、ここで強調しておきたいのは、「単に観察するだけ」では意味がなく、(b) や (c) につなげることが前提とされることである。

もっとも上記 3 種の行為は、それぞれが単独で（あるいは時差を以って）実行されることも多いだろう。そこで CISA は、法的免責を規定する部分では、個別に免責の可否を判断している[51]。しかし、本稿においてそれらの詳細を述べることは煩瑣に過ぎるので、以下では「モニタリング」で代表させ[52]、誤解が生じかねない箇所に限って (b) や (c) を区分して論ずることをお

---

[48] DM とは、既知または疑わしい脅威または脆弱性を探知・予防または軽減するために、情報システムと、システムに保存・処理・送信された情報そのものに適用される行為で、デバイス・手法・シグナチャー・技術・その他の方法をいう。ただし、他者の情報システムまたは情報そのものを破壊し、不正なアクセスを可能にしまたは重大な害悪を及ぼすものは除く（CISA Section 102 (7)）。

[49] CTI は、次の 8 つの態様を含むものとされる。① 脆弱性情報の収集などの偵察、② 脆弱性の利用の仕方、③ 脆弱性を前提にした特異な行動、④ ユーザの合法的アクセスによってセキュリティ管理を破る方法、⑤ 悪意の C&C（Command & Control）、⑥ 秘密裏に盗み出された情報など顕在・潜在の被害、⑦ 法によって禁じられていない、その他の特性、⑧ これらの組み合わせ（CISA Section 102 (6)）。

[50] CISA Section 102 (13)。

[51] 例えば、モニタリングの範囲を超えた DM 措置には、免責が及ばないとする以下の注意書きを参照。Note that there is no similar liability protection for operating defensive measures that go beyond monitoring.
（https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/, p1）

[52] モニタリングに関する CISA104 条の以下の規定は、以下の通りである。
AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS
SEC. 104. [6 U.S.C. § 1503]

許し願いたい。

モニタリングの権限と責任は、1960 年代に登場した provider exception（PE）という概念に端を発し、徐々に発展してインターネットにも cyber-trespass（CT。より詳しくは後述の Trespass to Chattel）として適用されるようになったとされる。刑事法分野での論客として知られる Kerr は「米国で最も広く読まれている法律関係ブログの1つ」（Wikipedia の評価）である Volokh Conspiracy のブログで、次のように述べている[53]。

> The idea for the provider exception first arose in the 1960s when the telephone company would listen in to fraudulent calls made by blue box users to try to identify the users. The provider exception was made statutory in 1968, and it was extended to the Internet in 1986[54]. ------But how the provider exception applies to the Internet has remained pretty murky.

Murky は、dark or dim、darkened or blurry とともに not clearly known, understood or expressed と説明されている（https://www.thefreedictionary.com/murky）が、PE の評価として適切な表現であろう。実は、米国では CT に関して「故意に過大な負荷をかけることはサーバの所有者の property の権利を侵害する」という論理の妥当性が、現在もなお争われているからである。

3.2 Trespass の法理と背景にある property の概念[55]

このような事案で最も頻繁に使われる法理は、trespass to chattel（動産に対する侵害）という概念である。これは不動産に対する trespass（不法侵入）の法理を動産にも拡大したもので、現行の restatement[56] である Restatement（Second）of Tort では、‘intentionally-----dispossessing another of the chattel, or using or intermeddling with a chattel in the possession

---

(a) AUTHORIZATION FOR MONITORING.—
(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor— (A) an information system of such private entity; (B) an information system of another non-Federal entity, upon the authorization and written consent of such other entity; (C) an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and (D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.
(2) CONSTRUCTION.—Nothing in this subsection shall be construed— (A) to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this title; or (B) to limit otherwise lawful activity.

[53] https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/ なお、論文ではないブログを引用することに抵抗があったが、このテーマは現在も FCC の Open Internet Rules の一部として、なお議論が続いているので適切なものを見出しがたかった。議論の紹介としては、Ohm [2010]、Cannon [2012] などを参照。

[54] なお、PE の具体的内容に関しては、後掲注 60 における 18 U.S.C. § 2511(2)(a)(i) の規定を参照。

[55] 以下の記述は、主として共著者の 1 人である林のブログ「情報法のリーガル・マインド その日 その日（26）資本主義と property 信仰」（http://www.cyber-literacy.com/cll/category/k_hayashi/page/4、2018 年 9 月 27 日）に拠っている。なお「同（27）Intel v. Hamidi 事件再論」（11 月 6 日）も参照。

[56] 判例法の国である米国で、過去の判例から一般的法理を抽出し条文化することで、州などにおける立法の参考にする資料。

of another’（217 条）とされている。

したがって、侵害を主張する側は 1）故意、2）動産に対する介入、3）実際の損害を証明しなければならないが、このうち第 3 点は、不動産への不法侵入の場合は不要とされている。つまり、不動産の場合は損害が発生しないような侵入であっても、侵入それ自体が違法あるいは不法となる。

そこで property の外延を幅広く捉え「資本主義」の基礎であると考える傾向のある米国では、初期の判決として動産への介入であっても 3）を不要とする eBay v. Bidders’ Edge 判決（100 F.Supp.2d 1058 (N.D. Cal. 2000)）などがあった [57]。しかし、Intel v. Hamidi（30 Cal. 4th 1342 (2003)）以降は [58]、restatement の文言通り、「実害の発生が前提」との理解が浸透しつつあるかに見えるが、なお根強い property 重視派があって、「不動産侵害と同様、侵入行為自体が違法」という主張も続いている。

ところで慣習法の伝統がある米国においても、「通信事業者は通信の中身に手を触れてはならない」という規範（hands-off 原則）が、わが国ほど厳密に解釈されているわけではないにしても、後述（4.2）の PBC 分類として機能している。ここで CT を認めることは「サーバなどの資産の所有者が通過する情報を制御する」ことを認めることになり、hands-off 原則と両立しないので、法理論として両者の関係を明確にすることが必要であった。

Kerr は、2015 年サイバーセキュリティ情報共有法には、この点を明確にする役割が期待されていた、という。しかし結局のところ、明確化の役割は、今後判例において cybersecurity purposes の概念がどのように解釈されるかを待たねばならないとしている。CISA における「サイバーセキュリティ目的」の定義が、“the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability” と幅広いことから [59]、適切な評価だろう。

> In part because of this murkiness, Congress enacted the computer trespasser exception in 2001. ------The idea is that the provider exception only allows monitoring for the provider’s purposes, and that providers who lack the ability or interest to monitor hackers inside their networks may nonetheless be willing to consent to others monitoring those hackers. So 18 U.S.C. § 2511(2)(a)(i) allows the government to monitor hacker communications inside a victim’s network when the victim allows it and the government actor “ has reasonable grounds to believe that the contents of the computer trespasser’s communications will be relevant” to an ongoing investigation.[60] --------

[57] 事案は、eBay という最大のオークション・サイトに対して、まとめサイトを運営する Bidders’ Edge が反復・継続的なクロールをかけたのに対して、eBay が Trespass to Chattel で訴えたもので、判決は eBay の言い分を認め、実害の証明を不要とした。

[58] このケースは、Intel 社の社員であった Hamidi が不当に解雇されたとして、同社社員と OB 用メーリング・リストを使って同報メールにより、自身の立場への理解を訴えた行為（ただし受信を望まない場合は、送信停止はできる）が Trespass to Chattel に該当するかどうかが争われたもので、判決は実害が生じていないとして Intel の訴えを退けた。

[59] CISA Section 102 (4)。後段の記述は monitor の定義と、ほぼ似通っていることにお気づきだろう。

[60] わが国の通信傍受法に相当する Wiretap Act of 1968（後に法典化され 18 U.S.C. § 2511(2)(a)(i)）は、次のように規定して

> And it seems to allow monitoring for cybersecurity purposes generally, including outsourcing of that role to others, instead of limiting the exception to monitoring to protect the provider's own network. With that said, there is a lot that is unclear, especially with regard to what counts as a "cybersecurity purpose."

この経緯から読み取れる教訓は、モニタリングの正当化理由としては property 理論だけでは不十分であり、何らかの新しい根拠づけを必要としているということである。私たちは、この課題に第 5 章で取り組むことにしよう。

3.3 EU の NIS Security Directive

一方 EU では 2013 年早々から検討されてきた Directive on Security of Network and Information Systems（通称 NIS Security Directive）が、長い検討を経て 2016 年 7 月 6 日に欧州議会で可決された。これは加盟国に以下の義務を課すものである（林 [2017b]、島村 [2018]）。① NIS に関する国家戦略の策定、② 協調グループの設置、③ CSIRT（Computer Security Incident Response Team）ネットワークの構築、④ Operator of Essential Service (OES) と Digital Service Provider（DSP）に対するセキュリティとインシデント通知の要件を定める、⑤ 所管官庁、Single Contact Point（SCP）、CSIRT の指定。

この Directive は、28 か国（英国の離脱前）もある加盟国間に対応の差があることを認めた上で、SCP や CSIRT の指定など最低限の共有の仕組みを整えるとともに、わが国では「重要インフラ」として一括りにされる産業の中から、OES と DSP に特に注目して、セキュリティ対策とインシデント報告の義務を課している点が注目される[61]。

共有される情報の定義は「リスク（NIS に悪影響を及ぼす可能性があると合理的に特定可能な状況または事象）に関する重大な情報」であり、米国ほど細かく規定されていない。また情報提供者の定義として、OES とは「(a) 社会に不可欠なサービスを提供し、(b) サービス提供が NIS に依存し、(c) 事故がサービス提供に壊滅的な影響を及ぼす事業者」であり（4 条 4 項および 5 条 2 項）、DSP とは「デジタル・サービスを提供するすべての法人」とされている（4 条 5 項および 6 項）。

通知されたインシデント情報の扱いに関しては、以下のような規定がある。

(1) OES はサービスの継続に深刻な影響があるインシデントを、遅滞なく所管官庁等に通

いる。It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks. 同種の規定（文言が微妙に異なる）が、Stored Communications Act にもある（18 U.S.C. §2701(c)(1)）。

[61] ここで DSP を取り上げていることは、Google などアメリカ系企業にも、域内に本社があるか代表者がいる限り、同様の義務を課す意思を強調したものと思われる。

知する義務がある。提供される情報は、機密性が保たれる。受け取った側はフォローアップ情報を提供しなければならない。SCP は、影響を受ける他の加盟国に送付する。個別のインシデント情報が事故の予防等に役立つ場合には、提供者と協議して公表できる。

(2) 加盟国は所管官庁に、OES に対する次の権限を付与しなければならない。① セキュリティ・ポリシーの策定と提供、② セキュリティ監査結果などの証拠の提供。ただし、要求の目的を明記し、情報を特定しなければならない。

(3) DSP はサービス（オンライン・マーケット、検索エンジン、クラウド・コンピューティングに限る）の継続に深刻な影響があるインシデントを、遅滞なく所管官庁等に報告する義務がある。ただし、義務が発生するのは対象利用者・事故期間・地理的広がりなどを見積もり得る場合に限る。また提供される情報は、機密性が保たれる。なお、OES が依存する DSP の事故は、OES が報告しなければならない。

(4) 受領した所管官庁等は、影響を受ける他の加盟国に送付する。また個別のインシデント情報が予防等に役立つ場合には、提供者と協議して公表するか、公表を求める。

(5) 加盟国は所管官庁に、DSP に対する次の権限を付与しなければならない。① NIS セキュリティを検証するための情報の提供、② 必要なセキュリティ・レベルに達していない場合の改善。なお DSP が、加盟国に複数の施設か代表者を置いている場合は、主たる施設か代表者の加盟国が、他の加盟国と相互に協力する。

(6) DSP に関する規定は、小企業・零細企業には適用しない。

EU 型の特徴は、28 か国の統一指針を作らねばならないことから、かなり細かい手続きを決めた点にある。しかし国家安全保障やインテリジェンス活動は、加盟国に固有の権限として留保されていることから [62]、EU 側で提供できる情報は少なく、民間企業にインシデント情報の報告義務を課すことになっている。そのような中で、米国系企業に席巻されている DSP に関して、域内企業と同等の義務を課していることが注目される。

3.4 英国・仏国の動きと GDPR

Edward Snowden による大規模なインテリジェンス情報の暴露（2013 年）や相次ぐテロ事件を経て、各国とも人権の保護と情報監視活動のバランスに関して、より深く考えるようになるという、大きな変化があった。

中でも英国は、従来インテリジェンス情報の収集をほぼ行政裁量に委ねてきたが、2016 年に「調査権限法」（Investigatory Powers Act = IPA）を制定して、独立行政委員会である IPC（Investigatory Powers Commissioner）の下にチェック機能を統合するとともに、IPC 内部に裁判官の資格を持つ委員を置き、令状を事前審査することとした。これは、手続き面で米国型に

[62] この点で、軍事情報に関する限り、NATO の役割にも目配りする必要がある。

やや近づきつつも、従来の情報活動をほぼ全面的に踏襲するものと理解することができる（情報セキュリティ大学院大学 [2017]）[63]。

仏国は、2015 年に「情報監視活動法」を制定して、国の情報活動の規律を定めた。仏国は従前、個人の自由と権利に関する意識が高く、「情報専門機関の活動のための一貫した完全な法的枠組みが西欧先進諸国の中で最も遅れている国の1つ」と自覚していたので（豊田 [2017]）、この変化は注目される。

また同国は、2016 年のデジタル共和国法によって郵便・電子通信法典を改正して、「通信の秘密は、通信の内容、通信当事者の身元（identité）、メッセージの表題及び通信に添付された文書に及ぶ」と範囲を明確にしたことが注目される。この規定は、添付ファイルにまで及ぶ点で秘密の範囲が広いが、わが国で通信の構成要素全般や、通信の存在の有無まで含まれると解されていること（前出 2.1 および 2.2 と、注 25 および 26 を参照）と比較すると狭いことになる（曽我部 [2019]）。

ただし、通信の秘密とは別に、「トラフィック・データ」「技術的データ」が、通信における私生活の保護の一環として保護される。従ってアンバンドルの観点からすれば、「通信内容」と「ログ」、「通信の秘密保護」と「プライバシー保護」が、従来以上に明確に切り分けられ、分節化されたことになる。

また、通信の秘密の例外事項として、a) 利用者の同意なしに「通信の秘密」に属する情報が利用可能な場合と、b) 利用者の個別の同意があれば利用可能な場合が明記された。a) において、通信の表示・分類・ルーティングのため、または迷惑メールやマルウェアの検出のために、自動処理により分析することの妨げにならないとの規定が置かれたことが注目される。これは、米国の CISA とともに、サイバーセキュリティに対処するための正当行為を明確にした点で、本稿の議論に有益な示唆を与えるものと思われる [64]。

このような英仏の変化とともに、EU 全般に関していえば、個人データ保護に関する GDPR（General Data Protection Regulation、2016/679(EU) of 27 April 2016）への関心が高まっているが、これは本来「刑事司法指令」（2016/680(EU)、GDPR と同日施行）、「e プライバシー規則」（最終案を検討中）とともに 3 点セットをなすものである（石井 [2020]）。

その意味で、刑事司法指令に「個人データの保存および見直しの期間制限」が含まれていること（第 5 条）と、「個人データの取り扱い業務に関する（ログまたは他の記録形態での）法的根拠の表示と記録が義務付けられている」こと（第 24 条）は、既に指摘したように（1.1 節）ログの利活用が手続きの正当性の根拠になっていることを、裏付けていると思われる。

---

[63] 手続き面での人権侵害への配慮を強める一方で、スノーデンが糾弾したインテリジェンス機関による情報収集の手段については、従前のものをすべて是認しているからである。

[64] なお曽我部 [2019] は、b) において広告・統計・サービス改善のために利用する場合には 1 年毎の個別の同意を取れば可能という道を開いていることは、行動ターゲティング広告のあり方にも関連すること、また e プライバシー規則の導入によって、国内法制に変化があり得ることに注意を喚起している。いずれも重要な指摘であるが、本稿のテーマからはやや外れるので、付言するに止めておこう。

3.5 わが国における「サイバー関連事業者」の責務

このような先進諸国の動きに対応して、わが国でも 2014 年にサイバーセキュリティ基本法の制定により、重要社会基盤事業者やサイバー関連事業者などの概念が導入され、その基本的な役割が規定された。また、同法の 2019 年の改正ではサイバーセキュリティ協議会の規定が追加されている。こうした規律の背景は、以下のように理解することができる。

インターネット以前のネットワークは、電気通信事業者など専業者によるものが大半だったし、情報システムと接続するのはごく一部に過ぎなかったので、ネットワーク管理の権限と責任は電気通信事業法 [65] に規定されたもので十分と考えられた。しかし、現代の主たる通信手段となったインターネットは、利用者が自ら運用する自律システムの相互接続が前提であり、誰がどのような権限を持ち責任を負うのかは、必ずしも明確ではなくなっている（田川 [2013]）。

インターネットが倫理観に富んだ研究者のネットワークであった時代には、このような制度の不備が顕在化することはなかったが、サイバー攻撃が日常化した現代では、何らかの形で情報ネットワーク・システムを所有する者や利用する者のうち主要なプレーヤーについて、権限と責任を明確化することが望ましい。この点で画期的と思われるのは、サイバーセキュリティ基本法が 6 条の重要社会基盤事業者の責務に加えて、7 条でサイバー関連事業者その他の事業者の責務を、表 7.のように定めていることである。

表 7. サイバーセキュリティ基本法におけるサイバー関連事業者等の責務

サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

ここでサイバー関連事業者には、「インターネット等その他の高度情報通信ネットワークの整備」を行う電気通信事業者、「情報通信技術の活用」者として情報サービス事業者やクラウド事業者、「サイバーセキュリティに関する事業を行う」MSSP（Managed Security Service Provider）などセキュリティ事業を受託して行う事業者やセキュリティ機器やソフトなどを製造・販売するベンダ、あるいはそのインテグレータ等が該当するのではないかと思われる。また「その他の事業者」は、オン・プレミスで情報システムを所有（運営を委託する場合を含む）する一般企業と解釈できる [66]。

しかしサイバーセキュリティ基本法は、その範囲を明記せず、インターネットを利用するすべての企業が含まれてしまうような漠然として規定になっている。これは一面で、どのような組織も

[65] より厳密には、その前身である公衆電気通信法というべきかもしれない。
[66] 本法は議員立法であるためか、逐条解説や立法趣旨説明などの書物が公刊されていない。

反復継続的にコンピュータを利用していれば「その他の事業者」になり得ることから [67]、個人を除いたすべての組織の権限と責任（権利の面と責任の面はバランス良く規律されるべきであり、本稿では「対になるべき概念」として使用する）として定めた結果になるという利点も有している。

しかし他方で、「誰に宛てたものか不明確である」「権限と責任が明確にされていない」という欠点も内包している。サイバー空間の安全対策は政府と事業者と利用者が一体となって推進しなければ実効性を担保できないことを考えれば、「サイバー関連事業者その他の事業者」のうち少なくとも前者については、権限と責任の明確化が必須であると思われる。

この点は、わが国の「サイバーセキュリティ戦略」と密接な関係があり、表6．はその結果ともいえる。2015 年以降に策定され始めたわが国の戦略には、① 平和国家にふさわしく積極的サイバー防御（Active Cyber Defense = ACD）などの攻撃性を示唆する手段には極めて謙抑的であり、② 同じコインの裏側として、政府の出番が少なく民間部門の対策が中心になっている、という 2 つの特徴がある。これは、サイバーセキュリティにおける、わが国の過去の蓄積の乏しさを反映した面があるので、早急に改革することは難しい。

私たちが表 6.のような分類を提案し、さし向き第 5 段階までの改善策を検討することで自制しているのは、まさにこのためである。そして、逆に自ら限界を設定すればこそ、ぜひとも実現しなければならないと考えている点が、「自律システム」の特性と重要性に関する理解を共有してもらうことであり、その基本動作がネットワーク・システムのモニタリング・自己防衛へのログの利活用・インシデント報告・インシデント情報の共有である。

コンピュータと通信ネットワークが、分かちがたく結びついたインターネット [68] においては、それぞれの管理システムは別であっても、「自律システムのセキュリティ管理システム」として共通要素を含んだものになっている [69]。また、ログという語が通信ログ（更に細分すれば、接続認証履歴など）からイベント履歴まで、メタ情報（情報を伝達・処理・記録・検索する際に必要となる「情報に関する情報」）として、そうした管理の不可欠の要素になっているからである。

3.6 重要社会基盤事業者のインシデント報告義務

前節で論じたサイバー関連事業者のモニタリング義務とともに、EU で実施中の OES に対するインシデント報告の義務化も、有効な手段である。サイバー対策の策定には、できるだけ詳細で、できるだけホットなインシデント情報の入手が不可欠だからである。NIS Directive は、その点で手本になると思われるが、そこには 3 つの配慮が必要である。

まず第1は、情報の集約ポイントである。わが国においては、電気通信事業をはじめ業法において当該義務化がなされていることが多いが、これらの情報は所管官庁に報告されるため、

---

[67] 法律における「業として」の定義は、「反復継続性と事業的規模の両方を満たすもの」とされており、後者は「社会通念上『事業の遂行』とみることができる程度のもの」をいう（吉国ほか編 [2009]）。

[68] NEC が Corporate Identity に近い用語として使っていた C&C（Computers and Communications）の方が的確な表現かもしれない。

[69] SIEM（Security Incident and Event Management）では、両者を統合することが前提になっている。

所管外の官庁が利用できるようにするには工夫が必要である [70]。最近では官庁間のサイバーセキュリティの相互連携が強化されたとはいえ、縦割りの弊害が払拭されたとは言えず、改善が必要であろう。

第 2 点は、義務化する対象企業の範囲である。EU のように OES という新たな分類を検討する方法もあるが、わが国には「重要社会基盤事業者」という概念があり、それなりに横通し（例えば、定期的会合や合同演習など）も行われているので、これを生かすのが早道であろう [71]。

第 3 は、報告されるインシデント情報が「詳細でホット」であることを、どうやって担保するかである。これは、本来ならモニタリングと一体になって、初めて意義があるものと思われる。一般的なインシデント情報は、攻撃が行われた後で得られるのに対して、モニタリングでは「現在進行形の情報」が得られる場合があるからである。

3.7 インシデント情報の共有

残念ながらサイバーセキュリティにおける「攻撃者優位」の状況は、当分変わりそうにない。そこで被害を受ける側の対抗策として最も期待されるのは、関係者間の情報共有と協調行動である。

業界団体や、セキュリティ関連の NGO、あるいは政府関連の組織等と通じたインシデント情報などの共有は、ISAC（Information Sharing and Analysis Center）、JP-CERT/CC（Japan Computer Emergency Response Team/ Coordination Center）、IPA（Information Promotion Agency）、JC3（Japan Cybercrime Control Center）などを通じてボランタリーに行われてきたが、サイバーセキュリティ協議会の発足に伴って、一段と強化されたかに思われる。今後は協議会の参加者の間の情報共有を 1 つのモデルとして深化していくことが期待される。

その基本は、a) サイバーセキュリティの確保は、本来各組織が自主的に取り組むべきものではあるが、b) サイバー攻撃の複雑化・巧妙化により、被害組織（被害組織から相談を受けるセキュリティ・ベンダや専門機関等を含む）が単独で有効な分析を行い、確証をもって効果的な対策を迅速に講じることに限界が生じてきており、c) 被害組織等から他の組織へ迅速な情報共有が行われなければ、攻撃手口や対策手法等を他組織が知ることができず、同様の手口によるサイバー攻撃の被害がいたずらに拡大するおそれがある、との認識に立っている [72]。

---

[70] 電気通信事業においては、電気通信役務の提供を停止又は品質を低下させた事故のうち、電気通信事業法施行規則第 58 条第一号に掲げる基準を満たす場合には「重大な事故の報告」を、影響利用者数が 3 万人以上又は継続時間が 2 時間以上の場合には「四半期報告」を行う必要がある。

[71] 現在「重要社会基盤事業者」として指定されているのは、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット、石油の 14 分野である。

[72] https://www.nisc.go.jp/conference/cs/kyogikai/index.html 掲載の資料による。

第 2 部　電気通信事業者の自律システム管理責任と通信ログの役割

4　　自律システム管理責任の電気通信における意義

4.1　わが国における電気通信事業の設備規律

第 1 部ではネットワーク・システムのモニタリングがサイバー対策の起点になり得ることを指摘したが、この点に関するわが国の規律は、どうなっているのだろうか。既述の通り「通信の秘密」（事業法 4 条）の規定は、おそらく世界で最も厳格に解釈され運用されてきた（インターネットと通信の秘密研究会 [2013][73]）から、hands-off が第一原則であることは明らかで、この限りではモニターは許されないだろう。

特に、米国では Provider Exception の概念が認められてきたのに対して、わが国にはそのような議論がなされてこなかった点は重要である。しかし他方で、わが国の事業法 41 条から 49 条は「電気通信事業の用に供する電気通信設備」の規律として、以下の諸点を定めていることも忘れてはならない。

a) 総務省が定める技術基準への適合性の維持（41 条・41 条の 2）、
b) 適合性の自己確認（42 条）、
c) 不適合の場合の総務大臣の適合命令の発出（43 条）、
d) 管理規程の策定義務（44 条）、
e) 要件不備の場合の総務大臣の変更命令（44 条の 2）、
f) 電気通信設備統括管理者の配置と役割と解任（44 条の3、44 条の4、44 条の5）、
g) 電気通信主任技術者の配置・資格・試験・義務・解任など（45 条～49 条）。

加えて「設備の適正な維持管理」の規定は、業法を超えて有線通信と無線通信の一般法である有線電気通信法と電波法にも見出されることに注意を喚起したい。前者においては、「通信の秘密」（有線法 9 条・14 条）と同時に「技術基準」（5 条）、「設備の検査」（6 条）、「設備の改善措置」（7 条）などが求められ、後者においては同じく「通信の秘密」（電波法 59 条・109 条・109 条の 2）と並行して、そもそも無線局を開局するには厳重な審査があり（4 条～27 条の 17）、登録を経なければ運用できず（27 条の 18～27 条の 34）、無線設備が具備しなければならない技術条件も詳しく規定されている（28 条～38 条の 2）。

[73] http://lab.iisec.ac.jp/~hayashi/20130608Report.pdf

これらの規定から読み取れるのは、「（事業用はもとより設備の設置者が自ら使用する場合も含めて）電気通信設備を提供する者には、その公共的性格に鑑みて、適正に維持する権限と責任がある」ことを意味するものと思われる。しかもサイバー攻撃が日常的になった今日では、「設備の故障を最小限にする」という意味にとどまらず、「サイバー攻撃の被害からシステムを守る」という面での権限と責任が含まれるようになった、と解すべきであろう。

加えて、かつては「適正な維持管理」といえばハードウェアが主体であったが、今日ではソフトウェアが含まれるのみならず、ソフトの比重が高くなっていることに留意しなければならない。1990 年代後半に広まった、いわゆる「ワン切り」に対して、最終的には有線法の改正（15 条）で対処した経緯を想起させる [74]。

この意味では、記述が簡明な有線法 5 条の規定（1 項で技術基準への適合性を求め、2 項でその具体例として「他人の設置する有線電気通信設備に妨害を与えない」「人体に危害を及ぼし、又は物件に損傷を与えないようにする」の 2 点のみを掲げる）が、悪意のあるソフトであるマルウェアに対して、対抗手段を取る十分な根拠となり得るか否かを手始めに、法整備の全体を再検討する必要があろう。

このような比較をする限り、わが国の法制の基本的発想は、米国の CT の考えと著しく乖離するものではなく、潜在的には同様の理解を内包しているものと思われる。

4.2 メディアの規律に関する共通原理の不在

ところで電気通信も広義のメディアの一種であるから、その規律が他のメディアとの比較においても妥当なものであることが望まれる。メディアは何らかのメッセージを運ぶための手段であり、メッセージは原則として「言論の自由」の観点から保護されるべきものとすれば、メディアに関しては公的干渉が極力少ないことが望ましい。

しかし「憲法修正 1 条」を重視する米国においても、「情報を運ぶメディアと、そこで運ばれる情報に関する法的責任」に関しては、技術的制約と歴史的事情から、メディア毎に違った規律が適用されてきた（プール [1988]）。つまり、インターネット以前の主要メディアには、「新聞・出版（Press）」「放送（Broadcasting）」「通信（Communications）」の 3 分野があったが、これらに対する法的規制は対照的ともいえるものであった。

この 3 者の規律を、経済的規制（参入・退出や、料金規制など conduit に関する規制。以下 Cd と略記）と社会的規制（content に関する規制。以下 Ct）の 2 つの面から分類したのが表 8. であり、これは林 [1984] が定式化し PBC 分類と呼んだものである。表が示す意味を箇条書きにすれば、以下のように要約される。

[74] 電話機の呼び出し音を 1－2 回鳴らしてすぐに切り、相手の着信履歴に自分の電話番号を残すための手法。表示画面に「着信あり」と表示されるため、着信履歴に表示された電話番号に折り返し電話させ、相手に通話料を負担させることに加えて、折り返しの電話に音声ガイダンスなどを聞かせ、あたかも高額のサービスにつないだように見せかけ、指定した口座に金を振り込ませるなど悪質で社会問題になった。

表 8. 放送・通信・情報処理産業に対する経済的・社会的規制（PBC 分類）

社会的規制（Ct） / 経済的規制（Cd）	あり	なし
あり	放送（Broadcasting 型）	通信（Communications 型）
なし	C´型または Internet 型 ？	新聞・出版（Press 型）

① 最も古いメディアである新聞・出版（P 型）には、Ct 規制も Cd 規制もないので、「言論の自由を最もよく保障している」ものと理解されてきた（Marketplace of Ideas も [75]、これを念頭に置いたものと考えられるし、初期のインターネットもそのように期待されていた）。

② この対極にあるのが放送（B 型）であり、Cd 規制（電波の割り当て）Ct 規制（番組編集準則）の両面の規制を受けるが、これは「電波の希少性説」か、「メディアの部分的規制説」に根拠があるとされ [76]、「規制によってこそ公共の福祉が実現される」ものと理解されてきた。

③ この両者に対して通信（C 型）は、参入規制と料金規制という Cd 規制は受けるものの、Ct 規制は受けない（というよりも、そもそも通信の内容にタッチしてはならない）ものと理解され、「通信の秘密」は、この分野に特有の責務とされてきた。

④ 情報処理は Cd 規制も Ct 規制もないので、P 型と同じであるが、コンピュータの発展の初期段階における利用形態はバッチ処理であり、これをメディアの一種とする発想がなかった。

⑤ ところがここに、PBC いずれの型にも収まらず、これらを融合した機能を持ったインターネットが登場したので、これをどの型に当てはめるか、あるいは新しい秩序を構築すべきか、検討する必要が出てきた。次節で述べる notice-and-takedown 法理は、こうした事態に対処するための工夫であるが、C´型と呼ぶべきか、それとも全く新しい Internet 型と位置付けるべきか、まだ定まっていない。

実は、林［1984］の出版の時点では、インターネットは研究者仲間のマイナーなネットワークに過ぎなかったので、⑤ は将来の課題としておくことで十分であった。しかしインターネットの進化とともに、この問題は次第に重要になってきたため、hands-off が原則の電気通信事業者等（C 型）も、違法あるいは不正行為が行われていることを知っており、または知るべきであった（knew or had to know）場合には、違法（不法）情報を流通させない措置をとることが期待される状態になってきた（林［2005a］）。つまり純粋の C 型ではなく、C´型あるいは I 型に変質しつつある。

[75] 有体物が市場で自由に取引され優れた商品が生き残る（市場原理）のと同じように、「言論」という財貨も市場取引を可能にすれば、優れた言論が選ばれていくはずだという超楽観主義の主張。
[76] PBC 分類が成り立つということ自体が示すように、一部のメディアが規制を受けても他に自由なメディアがあることで、全体として「言論の自由」は担保されるとする説。

4.3 プロバイダ責任（制限）法から自律システム管理責任へ

hands-off 原則が維持されていた時代に、「第三者がネットワーク上にアップロードしたコンテンツが社会的に不適切である場合に、コモン・キャリアは責任を負うべきか」という議論が発生した。この問題に正面から応えようとしてのが、プロバイダ責任（制限）法[77]であった[78]。

これは、プロバイダ（電気通信事業者でもある）が、著作権侵害や名誉毀損に該当する情報や、いわゆる有害情報等がアップロードされたことを知って以降は「我関せず」を貫徹することができず、当該情報の削除等が求められることを前提に、その義務と免責の範囲を明確にした最初の法律である。

そしてサイバー攻撃が日常化した今日では、その対象に「ネットワークの機能に悪影響を与えるマルウェアが送信あるいはアップロードされたり、情報システムが攻撃された場合に、それを駆除・復旧するためにコモン・キャリアがどこまで関与できるか、あるいは関与すべきか」という論点が含まれるようになった。

このような歴史を総括すれば、「インターネット時代には、コモン・キャリアの責務とされてきた hands-off 原則は事実上修正されている」（林・田川 [2019]）と見るのが、適切な見方だろう。前者において、その原則を修正する法理が notice-and-takedown であり、後者における法理はまだ発展途上であるが、インターネットの基本原理である「自律システムの相互接続」というアーキテクチャには[79]「当該システムのセキュリティの確保は自己責任の範囲内」ということが含意されているのだから、当然の帰結であると考えられる[80]。

この意味では、米国の CISA は後者の法理を初めて明確にした先駆的な仕組みではあるが、新しい枠組みを創設したわけではなく、現状に合わせて法を制定したと見る方が当たっている。わが国もこれに倣って、「ネットワークとシステムおよびそこに保存されている情報の機密性・完全性・可用性を確保することは[81]、サイバー関連事業者の権限でもあり責任でもある」ことを、法的に明記することに意義があるのではないかと考える。

インターネットの時代には電気通信事業者だけではなく（もちろん、システムの規模や社会的影響力から見て、枢要なシステムであることは疑いないが）、AS 所有者すべてに自らのシステムを防御する権限と責任とがあると考え、これを「自律システム管理責任」と呼ぶことにしよう。

---

[77] 正式名称は「特定電気通信役務提供者損害賠償の責任の制限及び発信者の情報開示に関する法律」（2001 年法律第 137 号）。なお略称は「プロバイダ責任制限法」とする向きが多いが、後述のように本法が「免責」の根拠法であるとの理解よりも、「新たな責任」を創設したと受け取る向きが多いので、私たちは本文のようにカッコ付きで記している（林 [2005a] 以降）。

[78] もっとも、この法律においても「通信の秘密」に関する厳格解釈の影響を受けてか、発信者情報開示手続が厳しく、プロバイダに対する IP アドレスの開示請求と、当該 IP アドレスの該当者の電話番号等の情報開示の 2 段階が必要で、コストと時間の制約があった。ネット上の誹謗中傷により被害者が自殺するという異常事態を経て、その手続き改善が現在総務省で検討されている。

[79] 現代社会が高度の技術に支えられている以上、社会システムを支える制度もアーキテクチャに依存せざるを得ない。この点を最も早く指摘したのは、レッシグ [1999] であった。松尾 [2017]も参照。

[80] 米国では「サイバー事案における攻撃と防御の非対称」を解消すべく、「積極的サイバー防御」（Active Cyber Defense）が主張されているが、そこにも「自己責任」の発想がある（林・田川 [2018]）。

[81] 機密性（Confidentiality）・完全性（Integrity）・可用性（Availability）、略して CIA は、セキュリティの 3 大要件だとされている。

4.4 ISP に代表される電気通信事業者の役割

自律システム管理責任は、情報システムを所有する「すべての組織」に適用されるものであり、これには電気通信事業者や ISP（Internet Service Provider）も含まれるだけでなく、彼らにとって特別の意味を持っている。なぜなら日米を問わず、ISP に代表される電気通信事業者は伝統的なコモン・キャリアの類型に属し、「通信の中身にタッチしない」 hands-off の義務を負っていると解されてきたが [82]、上記の新規定はサイバーセキュリティに関する限り、その修正を求めるものだからである（林 [2005a]、林・田川 [2019]）[83] [84]。

サイバーセキュリティ対策において、電気通信事業者の果たす役割は重要度を増している。もちろん既知のマルウェアに対してエッジにあるデバイスでセキュリティ対策を施すこと（エンド・ポイント・セキュリティ）や、ネットワークとシステムの境界線におけるセキュリティ確保（ファイヤーウォール等）は必要である。

しかし 2010 年代以降のサイバー攻撃は、強力な組織（国家やそれに準ずる者を含む）が意図的かつ長期的に取り組むもの（代表例として、Advanced Persistent Threat = APT）に変質しており、未知のマルウェアを迅速かつ大量に送付するので、エッジやウォールに到達するまで放置できないか、容易に貫通されるほど強力で緊急性の高いものになっている（林・田川 [2018]）。

このような期待に応えられるのは、情報処理事業者、電気通信事業者のいずれか、またはそれらの協調体制であるが [85]、情報処理事業者は伝統的に政府規制のない（非規制）産業として発展してきたので、hands-off のような制約から原則的に自由である。そこで、法的な側面の検討が必要なのは、主として電気通信事業者ということになる。そこで、以下の記述は電気通信事業者に焦点を当てて論じよう。

---

[82] わが国では、電気通信事業法 3 条の「検閲の禁止」、4 条の「通信の秘密」、6 条の「利用の公平」が根拠になる。米国では Communications Act of 1934 における Title Ⅱのコモン・キャリアの規定が適用されるか否かで、扱いが分かれる。コモン・キャリアの場合は 47 USC 201 条の「FCC による規制」、同 202 条の「差別的取り扱いの禁止」、同 605 条の「通信の不開示」などが適用される。このうちわが国の電気通信事業法3条と 4 条は、通信類似のサービスにも適用される（同法 164 条第 3 項）が、他の規定は非電気通信事業者には適用されない（米国ではコンピュータ通信には、事業規制はない）。

[83] 「電気通信事業者等」と表記すべきかもしれないが、紛らわしいので「等」は省略する。以下の説明における「電気通信事業者」には、狭義の事業者に加えて「適用除外電気通信事業者」も含まれるものと理解していただきたい。

[84] Hands-off を修正すれば hands-on になると考えがちで、本草稿の初期段階では私たちもその陥穽に陥っていた。しかし、電気通信事業の本質は「情報の媒介」にあるので、「情報の意味」には関与すべきでないという原則は維持すべきと思われる以上、その責任はあくまでも「間接責任」にとどまるので、hands-on という表現は避けるべきであろう。

[85] 2020 年 7 月に公表された「IoT・5G セキュリティ総合対策 2020」においては、従来の「ネットワークと端末は別々の機能を持つので、セキュリティに関してはそれぞれが努力すべし」という態度から、「通信はネットワークを介してなされるのでもう少し通信事業者がアクティブな対策を取るべきだ」という姿勢への変化が読み取れ、本稿の立場とも合致するものと考えられる。

5 Notice-and-takedown 法理と自律システム管理責任

5.1 コンテンツに関する間接責任

インターネット商用化後も、技術が初期段階にあった時点では、電気通信事業者に hands-on を期待することは忌避されていた。しかし、前述の PBC の 3 分野にまたがったり、これらを超えるサービスが I 型に分類されると、「最も規制が緩いルール」である情報処理のルールの適用（表 8. の範囲外で、一切の規制がない）に傾くため、極言すれば「無法地帯」になりかねないという懸念が生ずる[86]。そこで先進諸国では 20 世紀から 21 世紀への変わり目あたりから hands-off を変更して、一定の条件を満たせば、電気通信事業者にもコンテンツに関して間接的な責任を負わせるようになった。

わが国の場合は 2001 年の「プロバイダ責任（制限）法」の制定がそれに当たり、プロバイダは「違法・有害情報」を放置すべきではなく、所定の手続きに従って送信防止措置を取るべきことが期待されている[87]。なお、わが国の法制は、著作権侵害と名誉毀損などの違法情報への対応、更にはいわゆる「有害情報」対処の三者を区分せず、同じ法律を適用することとしているが、米国では著作権侵害が別建てとなっている（平野 [2014]）[88]。

ここで notice-and-takedown 法制を導入したことは、その後の青少年保護法制（2008 年の青少年インターネット環境整備法など）において、いわば「情報媒介者の責務」として一般原則化されている（林・田川 [2019]）[89]。EU においても Electronic Commerce Directive 2000 において類似の規定がおかれ、著作権侵害のみならず、名誉毀損や違法・有害情報の掲載などにも拡張されている。これらの事実は、米国においても EU においても、「コンテンツに関する媒介者責任」の法理として、notice-and-takedown 方式が定着しつつあることを示している。

PBC の混沌の中から、この法理が存在感を増しているのは、それなりの理由がある。「プロバイダ責任（制限）法」の制定趣旨は、プロバイダの責任を制限することであると説明されているが、ISP 等の当事者からは「新しい責任を生み出した」と受け取る向きが多いことが象徴的で

---

[86] 実際米国では、「インターネット非規制政策」と称して、「言論の自由」を貫徹しようという考えが 1990 年代に実施されたが（林 [2002]）、次第に「既存の法がサイバー空間にも適用される」という考えに収れんしていった。

[87] 1) 情報の流通によって他人の権利が不当に侵害されていると信じるに足りる相当の理由があり、2) 自己の権利を侵害されたとする者から理由を示して侵害情報の送信を防止する措置を要請された場合、3) 発信者に対し当該送信防止措置に同意するかどうかを照会し、4) 7 日を経過しても同意の申し出がなかったときは、送信防止を行っても損害賠償の責任を負わない（3 条 2 項）。

[88] デジタルミレニアム著作権法（Digital Millennium Copyright Act: DMCA）は、主にデジタル化された著作物の流通を想定し、これに対応するための規定を追加したアメリカ合衆国の著作権法の一部（1998 年 10 月成立、2000 年 10 月施行）。プロバイダが著作権者からコンテンツの著作権侵害を通知された場合に、はじめに当該のコンテンツを削除した上で、当該コンテンツを Web 上に発信したユーザへ削除した旨を通知する。発信者がコンテンツの削除について異議申し立てを行った場合、著作権者へ異議申し立てのあった旨を連絡し、発信者が 14 日以内に裁判を提起しなければ当該コンテンツを Web 上に復活させる（同法 512 条）。このように米国の法制は、単純な notice-and-takedown ではなく、notice-counternotice-and-takedown だと評する論者もいる。

[89] 「青少年が安全に安心してインターネットを利用できる環境の整備に関する法律」（2008 年 6 月 18 日法律 79 号）において、「特定サーバー管理者」（2 条 11 項）に「青少年閲覧防止措置」の努力義務（21 条）を課したのは、4.2 節で述べた C´あるいは I 型規制の象徴的事例と思われる。

ある。ここでは前述の通り、「違法あるいは不正行為が行われていることを知っており、または知るべきであった（knew or had to know）」場合には、電気通信事業者が「通信の秘密」を盾に「我関せず」と言っていられなくなったのである。

もっとも、その法的根拠を突き詰めると、意外に脆弱との感も否定できない（林・田川[2019]）。特に、児童ポルノのサイトをブロックする根拠が「緊急避難」だとするのは [90]、適用が長期化・常態化した現在では疑問視されても止むを得ないだろう [91]。何らかの形で正当化根拠を与える法制が望まれる [92]。

正当化根拠を考える上で参考になるのは、著作権における侵害主体論の限界である。米国の著作権法には「寄与責任」（contributory infringement）の規定があるので [93]、間接的な侵害者を訴えるための要件はかなり明確である。しかしわが国の著作権法には同種の規定がないので、「クラブキャッツアイ事件」最高裁判所判決 [94] が生み出した、いわゆる「カラオケ法理」を拡張的に適用する判例が増えている。これは、物理的な利用行為の主体（歌唱をする客）とは言い難いカラオケ店を、カラオケ店が有する「歌唱する客に対する管理（支配）性と、客の歌唱から生ずる営業上の利益」という二つの要素に着目して、規範的に利用行為の主体と評価する考え方である [95] 。

良く練られた論理であるとも、擬制が過ぎるともいえる。しかし現実のビジネスにおいて、この法理を適用する事例が増えるにつれて、「外国に居住する日本人がインターネット経由で、日本の TV 放送の録画を自ら指示してサーバ等に保管し、（外国で）視聴するサービス」を提供することまで侵害とされるようになったのは、論拠の曖昧さに伴う弊害と言わざるを得ない [96]。「寄与侵害」の規定がない状況下で、同種の効果を持つものとして「侵害主体」の外延を拡大したことが、最終的には利用者の利便を阻害する結果になったからである [97]。

この例が示すように、インターネットで世界が瞬時につながる時代には、制度の良し悪しが産業の競争力にまで影響するので、制度設計者にはそれなりの熟慮とインテリジェンスが求められる。しかし環境の変化が急速である状況下で、事態を放置することは「時間という資源の浪

---

[90] 児童ポルノが社会問題化したことを受けて、2009 年設立の「安心ネットづくり促進協議会」に参加した関係者が議論を戦わせた結果、刑法 37 条の「緊急避難」としてならば違法性が阻却される、との合意に達したものである。なお、現在のブロッキングの具体的手順については、http://www.netsafety.or.jp/blocking/を参照。

[91] 共著者の 1 人である林は、ブロッキングの運用を監督する組織の長を務めたことがあり、関係者の努力には敬意を払いつつも、果たしてそれでよいのだろうかという疑問を払拭できないでいた。

[92] 緊急避難は刑法の概念を借用したものだが、刑法は諸法の中でも最も謙抑的であることが期待されることに加え、「緊急避難」には「補充性」の要件が必要であるので、現状をそのまま是認することには困難があろう。法解釈の現状については、例えば山口[2015] 参照。

[93] 判例法の国なので、当初は判決から生まれた概念であったが、今日では連邦著作権法 106 条の「排他的権利」に含まれると解されている。要件は、次の 2 点である。The defendant having knowledge of a direct infringement; and materially contributing to that infringement.

[94] 最三小判 1988 年 3 月 15 日 民集 42 巻3号 199 頁。

[95] 上野達弘 [2006]「いわゆる『カラオケ法理』の再検討」紋谷暢男教授古稀記念『知的財産権法と競争法の現代的展開』発明協会、参照。

[96] カラオケ法理の成立から、まねき TV 事件判決（最判 2011 年 1 月 18 日 民集 65 巻 1 号 121 頁）およびロクラク事件判決（最判 2011 年 1 月 20 日 民集 65 巻 1 号 399 頁）に至るまでの変遷は、田村 [2019] pp. 289~311 に詳しい。

[97] 共著者がともに米国東海岸に在住していた 1990 年代前半のニューヨーク市では、日本企業が CATV のチャネルを時間借りして、日本で録画した番組を空輸し 1 日遅れで放映していた。視聴者の多くが「インターネット経由で日本のテレビが見られたら良いのに」と思っていたことは疑いない。それが 2020 年になって、やっと実現しようとしているが、この間の時間ロスはビジネス上甚大である。

費」に他ならないから、「限定合理性（bounded rationality）」しか持っていないことを自覚しつつ、誤りがあればすぐに引き返すことを前提に「難局を何とか切り抜ける」（muddling through）方途を工夫するしかないであろう[98]。

5.2 自律システム管理責任の適用範囲

そのような認識に立って、自律システム管理責任の適用範囲を検討しよう。notice-and-takedown 法理は「通信の秘密」に対する例外である「コンテンツに関する間接責任」の端緒とはなったが、サイバーセキュリティに対する措置までも想定したものではない。両者の目的等を比較すれば、表 9. のような著しい差がある以上、後者にはそれにふさわしい仕組み、すなわち「自律システム管理責任」を検討すべきであろう。

表 9. コンテンツに関する間接責任と自律システム管理責任

比較項目	コンテンツ（間接）責任	自律システム管理責任
目的	誰もが安心して利用できるネット環境の維持	情報システムやネットワークの安定的提供（CIA の確保*）
被害者	情報システム等の所有者以外の第三者が圧倒的	情報システム等の所有者自身の場合がある
望ましい対策	侵害の通知を待って、違法・有害情報の送信を防止	セキュリティ対策は、政府・企業・利用者が全体で担うが、中でもサイバー関連事業者に多くを期待
根拠・関連法規	Notice-and-takedown、プロバイダ責任（制限）法	自律システムの基本理念。ハード・ローに原則規定を置きつつ、安全対策基準などソフト・ローが中心
比較較量あるいは両立すべき価値	プライバシー・言論の自由・検閲の禁止と違法・有害情報の遮断（相互に矛盾することが多い）	個人データの保護・プライバシーの保護とネットワーク・サービスの安定的提供（両立することが可能）
実効性	氷山の一角しか把握できないが、行為者は個人が多く抑止効果は少なくない	組織的攻撃には対応できず、後追いを強いられている

（注）機密性（Confidentiality）・完全性（Integrity）・可用性（Availability）、略して CIA は、セキュリティの 3 大要件だとされている。

上表における違いの多くは、サイバー・インシデントが、以下の 6 つの特色を持つことに起因

[98] Bounded rationality は経営学者のハーバート・サイモンの用語。また muddling through を、田村［2019］は「漸進的試行錯誤」と訳している。

すると考えられる。

a) 自律システム（AS）は、その名の通り、システム内の規律はすべて AS 所有者自身の権限と責任とされており、一見すると外部からの規律は不要に見えるが、
b) ボット（bot）に代表されるように [99]、いつの間にか自律システムが悪意ある攻撃者に乗っ取られ、C&C（Command and Control）サーバに支配される例が多く、
c) その場合は、被害者であるASが踏み台にされて、他のASへの攻撃者に様変わりし、被害が連鎖的に拡大することになり、
d) 最初の被害者であるASは、自力でのシステムの復旧は可能かもしれないが、攻撃者に対する対抗手段を有するケースはさほど多くない上、
e) 自力救済は原則的に禁じられているため（林・田川 [2019]）、
f) 被害者・業界団体・サイバー関連企業・政府機関などの相互の協力によってしか、事態が改善できない [100]。

このような特色を与件として、自律システム管理責任を、システムの内外と管理手段の 2 つの軸で分類すると、表 10. が得られる。この表を使って、責任の範囲を画定することを試みると、「主たる対象」として網掛けした 3 か所、つまり「AS 内のインシデント原因の解明」「AS 内のインシデント解消のための防御措置」「AS 外とのインシデント情報の共有」のみが対象になることが示される。

表 10. 自律システム管理責任の適用範囲

AS の内外 / 管理手段	AS 内	AS 外
インシデント原因の解明	主たる対象	対象外
上記の解消のための防御措置	主たる対象	対象外
防御を超える対抗措置	禁じられている	禁じられている
インシデント情報の共有	対象外	主たる対象

なお、ここで 2 点付言しておきたい。1 点目は、表 10. は理解を容易にするため簡素化しているのでグレイゾーンは省略しているが、防御と対抗措置の関係は実は微妙なことである。特に ACD（Active Cyber Defense）という概念を認めると議論は複雑になるが、この点については林・田川 [2019] で詳しく論じたので、そちらを参照願いたい。

第 2 点は、本節の分析を 1.3 節におかなかったことである。その理由は、電気通信ネットワークは自律システムの一種であるが、伝統的な電気通信事業に携わってきた人々の間では、そのような理解が乏しいため、第 2 部として際立たせたかったからである。表9. と表 10. を連続

[99] robot の IT 分野における略語。人間による操作や作業を代替したり、人間の行為を模して人間のように振る舞い、自動的・自律的に行動するソフトウェアやシステムなどのこと（IT 用語辞典 eWord）。
[100] 災害時において自助・共助・公助がすべて必要とされることや、公衆衛生に準じた作業がサイバー空間にも必要だという議論（cyber hygiene）などに、端的に現れている。

して見ていただければ、私たちの意図を汲み取っていただけるかと思う[101]。

5.3 ISP の自律システム管理責任の理論的根拠

自律システム管理責任を電気通信事業者に求めることは、理論的な裏付けがあるものだろうか。共著者の 1 人である林は、2008 年ごろから「コミットメント責任」という名の下で、同種の責任論の先駆けとなる概念を追及していた。「コミットメント責任」とは、「事業者が、情報管理の取扱いに関する約束事を消費者に対して提示し、又は社会に対して宣言したにもかかわらず、それに違反することによって生ずる責任（法的責任を中心にしながらも、より広い概念としての責任、免責を含む）」である（林・鈴木 [2008]、林 [2017a]）。

しかし、この概念は情報の漏えいなどの「注意義務違反」のレベルを定める、民事的救済の尺度としては有効であっても、攻撃型に変容したサイバー犯罪に対する刑事罰を含めた尺度としては機能しない[102]。そこで、わが国では少数派であることを承知の上で、「法と経済学」的な考察を試みよう。先駆的な議論はやはり米国にあるので、Lichtman and Posner [2004]と、その反論として典型的な Harper [2005] を素材として採り上げる。

Lichtman and Posner [2004] は、サイバー関連事業者への期待の高まりを、「法と経済学」における「最安価結果回避者（Cheapest Cost Avoider=CCA）」の理論で説明できる、とする。インターネットが、いわゆる「違法・有害情報」で汚染されており、何とか正常化したいとの要望は強いが、誰がその責任を負うべきかといえば、「最も低コストで悪影響を回避できる者」というのは経済合理的だろう。その有資格者は、「プラットフォーマー」と呼ばれる GAFA のような大企業か、旧コモン・キャリアか、新興の ISP 以外に考えられない。

彼らは、出発点として CCA 理論に依拠しながら、その後の理論の発展を踏まえ、以下のように主張している。まず、「直接責任」が原則であることを確認し、a) 直接行為者を特定することが容易で、行為者に損害賠償の支払い能力がある、b) 取引コストが高くなく直接行為者（＝責任者）が契約により責任の全部または一部を移転することができる、の 2 つの要件を満たす場合には「間接責任」は不必要であるとする。

しかし彼らは、サイバーセキュリティのように上記の 2 条件が満たされない場合には、間接責任が有効になる場合があるとして、その必要性を以下の and 条件で判断すべきであるとしている。ア）責任を負う主体が不法行為を発見し抑止できる立場にある（control 条件）イ）当該主体に不法行為から生ずる外部不経済を内部化するインセンティブがある（activity level 条件）[103]。

---

[101] 本文の説明を補足すれば、1.5 節が「通信屋」と「コンピュータ屋」のメンタリティの差を、どちらかと言えば「通信屋」の視点で見ているのに対して、本節の考察は「コンピュータ屋」の視点から見ているともいえよう。

[102] 行政法の分野においては、例えば消防法 7 条における建築物の新築等の許可、認可若しくは確認の際の消防長又は消防署長の同意や、同 8 条における防火管理者の配置・消防計画の作成などが義務付けられている。これらは何らかのハードウェア（有体物）を前提にしたものであるが、そのアナロジーを追及するのも 1 つの方法であろう。他方で前節の本文で述べたサイバー・インシデントの 6 つの特色を深堀りして、サイバー・ハイジーン（注 100）の具体化を図るのも、チャレンジングなアプローチである。

[103] しかし彼らは、この 2 条件は「間接責任を正当化する and 条件でも or 条件でもなく、単なる前提条件に過ぎない」とする。

2004 年に執筆された彼らの主張は、通信品位法（1996 年制定）や [104]、デジタルミレニアム著作権法（1998 年制定）の解釈において、インターネット上に公表されたコンテンツに関して、少なくとも通信の媒介者である ISP には免責を認める主張と判決が圧倒的であったことに対して [105]、警鐘を鳴らす意味があったと思われる [106]。

彼らの主張は、a）違法・有害情報、b）著作権侵害情報、c）サイバーセキュリティ事案の三者を切り分け、a）はコンテンツに関するものなので原則として直接責任だが、上記の control 条件と activity level 条件が満たされる場合には、間接責任を問うことも是認すべきであること。b）と c）はコンテンツには直接係らないので別途の扱いとし、b）に関してはDMCA に従うべきこと、c）に関しては、自らのシステムの安全性を守る場合は直接責任であり、他者の委託を受けてモニタリング等をする場合には間接責任の 2 要件を満たす、としているものと推定される。

これは、もともと著作権侵害事案と名誉毀損等の事案を別法で処理している米国では、その延長線上にある当然の発想ともいえるが、林・田川［2019］が提案した「③　違法・有害情報に対処するケースと、インターネット・サービスの安定的提供を確保するためのサイバーセキュリティ対策を場合分け」する提案に一脈通ずるものでもある。

しかし表面的な近似性にもかかわらず、両者は全く違った角度から見ていることも忘れてはならない。Lichtman and Posner［2004］が上記のような結論になるのは、彼らの立論が「著作権には他の多くのアプローチがあり得るが、セキュリティの選択肢は少ない」などの 6 点に基づくもので [107]、「法と経済学」の原点である「誰に責任を負わせるかは経済合理性（のみ）で判断できる」という枠組みから外れていない。これに対して共著者は、経済合理性（rationality）とともに世論の動向など法的・倫理的な面（reasonableness）も考慮しているからである [108]。

Lichtman and Posner［2004］の主張に対しては、当然のことながら異論もある。その代表例と

---

[104] 1996 年に成立した米国の電気通信法（1934 年通信法を改正する法律）に含まれる、インターネット上でのわいせつ文書や画像などを規制する条項（Communications Decency Act: CDA）。インターネットなどを通じて、みだらで不快な情報を 18 歳未満の者に対して提供することを禁止したものだが、ネットワーク関連企業や個人・市民グループなどが、「表現の自由」を侵害するものとして訴訟を起こし、米国連邦最高裁判所は 1997 年 6 月に違憲判決を下した。しかし、編集権を行使する publisher と行使しない distributor を区別し、後者にはコンテンツに対する責任はないことを明確にした条文は違憲とされなかったので、その後 publisher か distributor かを中心に多くの裁判で争われた（平野［2014］）。なお、これがインターネット非規制政策からの転換であることについて、林［2020a］と注 44 を参照。

[105] Lichtman and Posner［2004］は当然のことながら執筆時点以前の判例しか検討していないが、その後も免責を幅広く認める判断が続いているという（平野［2014］）。

[106] それは彼ら自身の以下のまとめに、端的に現れている。‘Rather our aim is to challenge the recent trend in the courts and Congress away from liability and toward complete immunity for Internet service providers. In our view, such immunity is difficult to defend on policy grounds, and sharply inconsistent with conventional tort law principles. Internet service providers control the gateway through which Internet pests enter and reenter the public computer system. They should therefore bear some responsibility for stopping these pests before they spread and for helping to identify individuals who originate malicious code in the first place.’

[107] 6 点とは、a）著作権侵害の間接責任者は、インターネットの汎用性を反映して広く拡散（chain 化）する懸念がある、b）むしろマイクロソフトのような事業者の方がセキュリティ事故による外部効果を内部化（価格転嫁）しやすい、c）チェーンはいずれエンド・ポイントに達するはずで、サイバーセキュリティの場合、それは ISP になろう、d）著作権の場合、侵害サイトがキラー・アプリになっているが、セキュリティにはそのような特異な事情はなく、ISP には内部化のインセンティブがある、e）著作権の場合は property 保護の問題だが、セキュリティにはその要素は薄い、f）著作権には他の多くのアプローチがあり得るが、セキュリティの選択肢は少ない、の諸点である。

[108] もっとも、より根源的な差は、セキュリティ・インシデントの共有体制から来るものかもしれない。米国では、表 6. の発展段階の第 6 段階（最終段階）にあり、わが国が第 5 段階に足をかけたにとどまっているのとは、顕著な差がある。後述のスノーデンの暴露を待つまでもなく、米国の識者の間ではセキュリティ分野における電気通信事業者等の役割は、既知のことであったとも想定される。

して、ここでは Harper［2005］の反論を紹介しておこう。彼は以下の 6 点から、彼らの説は受け入れられないという。a) 近代法の原則は「行為者に対する過失責任」であり、注意義務のない者に責任を課す「間接責任」は、ごく例外的にしか認めるべきではない、b) ISP にモニタリングを認めると利用者のプライバシー侵害の危険が高まる、c)「熱心過ぎる（overzealous」ISP は情報の過剰削除に傾く恐れがある、d) 自律分散ネットワークであるインターネットはエンドにおける自助努力を原則にすべきである、e) エンド・ユーザの自助努力を助けるソフトウェア開発こそ関連産業を発展させる。

Harper［2005］の言い分は、もっともな点が多い。しかし彼の主張は、インターネット発展の初期に見られた「インターネット原理主義」に近く [109]、その後の環境変化を反映していないように思われる。サイバー攻撃の激化は、2010 年代以降に顕著になったものであり、ハーパーの理解を超えるものであったろう。それに対してリヒトマンとポズナーの方が、どれだけ正確な予想をしていたかは定かではないが、少なくともサイバー攻撃が持つ潜在的影響に関して、感覚的な脅威を感じていたかと思われる。

いずれにせよ、両者の論争が 2010 年代にはほぼ忘れられ、「2015 年サイバーセキュリティ情報共有法」における「サイバーセキュリティ対策における情報システム所有者等の権限と責任」に異を唱える論者がごく少数に過ぎないことからみても（林・田川［2019］）、サイバーセキュリティという困難な課題に応えるためには、Lichtman and Posner［2004］の方を選ぶのが better であることまでは、大方の合意ができたと考えられよう。

6 先進諸国におけるログの利活用とわが国の対応

6.1 先進諸国におけるログの利活用

先進諸国においてログの知得・利用がどの程度認められているかを見ていこう。情報セキュリティ大学院大学に設置した「インターネットと『通信の秘密』研究会」において私たちが調査した結果、先進諸国の「通信の秘密の運用実態」に関して、表 11. のような知見を得た（情報セキュリティ大学院大学［2014］Executive Summary）。

表 11. 先進諸国における「通信の秘密」（ログを含む）の運用実態

1) 「通信の秘密」は絶対的保障を受けるわけではなく、「公共の福祉」の観点から、より高位の法益があれば制限される場合があることは、共通した理解である。わが国も理論的には同じ理解に立っていると思われるが、実際の運用は極めて厳格で、明確な「違法性

[109] その核となっているのは、e2e で表される「インテリジェンスをネットワークに置くのではなくエンドに置くべきだ」という意味での「エンド・ツー・エンド原則」だと思われる。詳細は、Saltzer, Reed, & Clark［1984］を参照。

阻却事由」がない限り「通信の秘密」が守られるとしている点は、先進諸国の間では「保護の程度が高い」類型になろう。

2) 「公共の福祉」の観点から、通信傍受などが違法性を阻却されるケースは、大きく分けて (a) 事業者のネットワーク制御に伴うものと、(b) 公権力の関与に伴うもの、に 2 分される。後者はさらに、(b-1) 犯罪捜査に伴うもの、(b-2) 国家安全保障にかかわるもの、に分けられる。

3) このうち (a) について本調査では、ISP が関与する以下の 5 つの個別事項に関して、各国での実施状況・法的規定・利用者の同意の 3 点について、調査を行った。① 迷惑メールのフィルタリング（ブロッキング）、② 帯域制御、③ サイバー攻撃などに対する情報セキュリティ対策、④ 違法コンテンツサイトへのアクセスブロッキング、⑤ 行動ターゲティング広告。

4) その結果、これらの事項は調査対象のいずれの国においても何らかの形で実施されているが、「各国ともほぼ同じようなレベルで実施されているもの」と「実施されているが、ISP が関与する程度が異なるもの」がある。また関与を認める法的根拠や実際の運用についても、必ずしも各国で足並みが揃っているわけではない。

5) このように一般的な傾向が明確でない中で、各国の ISP の関与について強いて大きな分類をすれば、EU 型においては「ネットワーク中立性」が重視され、事業者の裁量が制限されているのに対して、米国型ではネットワーク事業者の自由度が高いという対照があるように思われる。なお、ここでネットワーク事業者というのは電気通信事業者に限らず、コンピュータ・サービス提供者を含めた概念であり、後者において営業の自由度が高いのは「インターネット非規制政策」を取ってきた同国の特徴と考えられる。電気通信事業者に限って言えば、米国型でも「ネットワーク中立性」の議論がある。

6) (b)に関する部分については、以下のような諸点が注目される。① 関与の目的は、犯罪捜査とテロ対策を含む国家安全保障の二つ、② 関与の方式としては、現に行われている通信過程に関与する通信傍受と、通信終了後に通信事業者等によって蓄積された情報（保存資料）へのアクセスの二つ、③ 関与の対象は、通信内容と、通信内容以外の通信に関わるトラッフィクデータ・通信データ・メタデータ・通信属性と呼ばれる情報および通信自体ではなく加入契約に基づいて得られる加入者情報の三つ、④ 関与の手続きとしては、裁判所の令状を必要とする司法傍受と行政機関・捜査機関の手続きで良い行政傍受に分かれている。

7) (b-1) の犯罪捜査に伴うものに関しては、サイバー犯罪対策で国際条約ができたように、 国際的な制度の調整（ハーモナイゼーション）が最も進んでいるが、法制度は現実の各国の風土の中に存在するものだから、傍受に関する社会的受容度によって、実際の運用面ではかなりの差がある。とりわけ「令状主義」を貫徹し司法傍受しか認めないか、一定の条件の下では行政傍受を認めるかは大きな差であり、前者しか認めないわが国は「最も厳格な令状主義」を維持していると考えられる。

8) (b-2) の国家安全保障にかかわるものに関しては、各国のナショナル・セキュリティに関する感度（センシビリティ）が反映している。国家安全保障に係るインテリジェンス活動のための公権力の関与は、通信傍受と保存資料へのアクセスの二つがある。また手続き的には司法傍受と行政傍受と呼ばれる二つがある。犯罪捜査の場合とは違って、各国とも裁判所の関与なしで（行政・捜査機関だけの手続きで）傍受や保存資料へのアクセスを認めているが、基本的人権を必要以上に侵害することのないよう、手続き的な担保の規定もおいている。

9) とは言うものの、権限が濫用される危険と背中合わせであることに、より配慮しなければならない。いみじくもスノーデン事件で明らかになったように、歯止めのない傍受・アクセスが行われる危険があるからである。各国とも手続き的な工夫に努力しており、インテリジェンス活動を一切止めよという声は少ないが、人権の保障にはなお努力が求められている。

10) 各国比較による日本の制度への教訓として、以下のような諸点を引き続き検討すべきかと思われる。①「通信の秘密」を第一義的な問題として論ずることの妥当性（他の視点での検討の方が適している場合があるのではないか）、② 事業者の正当行為（わが国の流儀では「違法性阻却事由」）を予め法定化することの妥当性と、その際に電気通信事業者や ISP の財産権を根拠とすることの妥当性、③ 公権力の関与に関しても、これを法定化することの妥当性。

この調査は 2013 年に実施されたが、通信の「内容」と「通信ログ」の両者を含めて広義の「通信の秘密」と解する（第 1 章の分類では、② のアンバンドルを考慮しない）わが国の法制を、暗黙の前提にしたものであった。従って、当然に通信ログを包摂したものであり、特に 3) 6) 8) 9) の各項はそれを前提にした分析になっているとも言える。また、第 2 期調査では公権力の「通信の秘密」への関与についての記述にウエイトがあって、本稿のテーマである第 5 段階における民間企業や電気通信事業者の役割の記述とは、ずれている感は否めないが、先進諸国の状況を大筋で理解するには十分であろう[110]。

6.2 わが国におけるログの利活用（特にバルク利用）

表 11. の 10)③ に関連する重要な知見として、わが国は通信傍受法[111]の制定（1999 年）と改正（2016 年）により、犯罪捜査（表 11. では b)-1）のために一定範囲の「通信の傍受」を認めているが、国家安全保障（b)-2）における利用の根拠法はないことが挙げられる。また通信内容とログを区分する発想がないため、犯罪捜査のためであっても、「通信内容」の傍受が一定の要件の下で認められたことの反対解釈として、ログの知得・利用については、より謙抑的

[110] 表 6. の第 6 段階になれば、犯罪捜査、反テロ対策、インテリジェンス活動の3分類の方がフィットするかもしれない。
[111] 犯罪捜査のための通信傍受に関する法律（1999 年 8 月 18 日法律第 137 号）

な運用になっているのではないかと思われる[112]。

しかし、ログの知得と利用が全く許されない訳ではない。ごく限られた範囲ではあるが法律やガイドラインにより、コンテンツに関する媒介者責任と自律システム管理責任の両面で、それぞれ表 12-1. と表 12-2. のように、ログの利活用が認められている[113]。しかも自律システム管理責任の場合には、特定データとしてのログだけでなく、一部バルクデータの知得・利用が認められる場合があることが注目される。

表 12-1. 電気通信事業者による通信内容とログの知得・利用事例（違法・有害情報等に関する「コンテンツに関する媒介者責任」の場合）

事例	発信者情報開示	自殺予告事案の警察への発信者情報開示
根拠	プロバイダ責任(制限)法 4 条	インターネットの自殺予告事案への対応に関するガイドライン
目的	違法・有害情報等の流通抑止	人命保護
知得内容	特定の発信者情報 （特定データ）	特定データ

（注）青少年インターネット利用環境整備法 21 条において、特定サーバー管理者（同法 2 条 11 項。コンテンツ・プロバイダや掲示板・ホーム・ページの管理者などが該当）は、電気通信事業者ではないものの、青少年閲覧防止措置を取る努力義務が課されており、その際ログを利用している。また電気通信事業者にも、フィルタリング・ソフトの提供などの協力義務があるが、自身では通信ログを利用しない。

表 12-2. 電気通信事業者による通信内容とログの知得・利用事例（「自律システム管理責任」の場合）

事例	迷惑メールの取扱い拒否	サイバー攻撃に対する対抗措置	特定のアプリやユーザの通信帯域の制御
根拠	迷惑メール防止法（特定電子メールの送信の適正化等に関する法律）	電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン	帯域制御の運用基準に関するガイドライン
目的	インターネット・サービスの安定的提供と受信者が希望しない e-	サイバー攻撃に対する通信遮断等	インターネット・トラフィックの制御

[112] 捜査関係事項照会の形で、ごく限られた範囲で利用されているに過ぎないものと推測され、照会書全体で年間 2 千件程度といわれるが、ログの照会がどの程度かは不明である。
[113] なお、2 つの表の内容は林・田川 [2019] と同じであるが、「インターネット・サービスの安定的の提供」を、本稿の用語である「自律システム管理責任」に改めるなど微修正した。

	mail の送信防止		
知得内容	メールサーバ上でバルクデータを知得して、迷惑メールリストとの照合により、取扱い拒否メールを抽出	特定データとバルクデータの両方の場合がある	通信経路上でバルクデータを知得して、特定ユーザなどの通信総量データをチェックして、帯域制御を行う

このように、「通信の秘密」に世界一敏感と思われるわが国で、一見意外にも思えるバルクデータの知得（そして、その一部の特定データとしての利用）が認められていることは、利用されるデータには個人情報を含まず、かつ人手を介せず機械処理することが、大前提になっているものと思われる。この意味で、「ログの利活用に関する 9 原則」（表 3. 第 1.4 節）の前提として、「semantic 的利用」と「syntactic 的利用」を分けたことは、それなりの妥当性を有しているかと思われる。

しかし、当該情報がデータとして保存されていれば、何らかの経路で流出する危険は残る。また、こうしたログのバルク利用が法律ではなくガイドラインを根拠にしている場合は、万一流出などが起きた場合の救済措置が、不十分であることも考えられる。この意味では、わが国の法制は、その根拠付けと人権保障の両面で、更なる透明化の要請を受けていると考えられる。

諸外国においてもログの利活用は、原則として発信者等を事前に指定した「特定データ」として許されるだけで、発信者等を特定しない悉皆的な「バルクデータ」としての知得を明文で認めているのは英国だけである（なお知得・利用できる者を、インテリジェンス機関に限っている。情報セキュリティ大学院大学 [2017]）。

しかし、これは英国が ISA（Intelligence Services Act 1994）などで、インテリジェンス活動に関してもなるべく法的根拠を明確にしようとしているからであろう。実行上は、他の先進国においても同様の機能を認めているが、その根拠を、例えば米国は大統領の憲法上の権限などにおいているため [114]、英国のような個別法は不要としているだけではないかと推測される [115]。

現に、かつてはインターネットのアーキテクチャ的制約から、サイバー攻撃の実行者の特定（いわゆる attribution 問題）の解決は不可能で、「攻撃者が防御者より優位」という事態は変わらないと見られていた。しかし 2010 年代に入って米国は、膨大な資金と人的資源を使って官民協力による刑事訴追の努力を続けた結果、中国人民解放軍の幹部や北朝鮮のクラッカーなどの訴追に成功している（林・田川 [2018]）。起訴状（criminal complaint）では限定的な証拠

[114] 米国憲法における「行政権は合衆国大統領に帰属する（第2条第1節第1項）」との規定や、大統領が「軍の最高司令官（Commander in Chief）である」（第 2 条第 2 節第 1 項）ことなど。

[115] 米国は EU との間の個人データの越境的利用手続きに関して、EU 司法裁判所の無効判決を受けた safe harbor 条項では不十分であるとの EU の主張を入れて、2016 年から privacy shield 方式に改めた（林・田川 [2016]。しかし、これまた 2020 年 7 月に無効判決を受けている）。これと相前後して USA Patriot Act of 2011 の 215 条が時限切れとなり USA Freedom Act of 2015 に引き継がれた際、バルクデータの収集は禁じられた。しかし、NSA がユタ州に建設した巨大なデータ・センターが稼働を始めたことからみても、別の形でのバルク取得は続いているものと考えざるを得ない。https://en.wikipedia.org/wiki/Utah_Data_Center 参照。

しか示されていないので全貌を理解することが難しいが、インテリジェンス情報抜きで、このような行動が可能になったとは思われない[116]。

インテリジェンス活動は、近代兵器を駆使した第 2 次世界大戦下で活発化したが、終戦後は主対象国をソ連に絞って「ひっそりと」引き継がれていった。特に通信傍受等に携わる米国の NSA（National Security Agency）や英国の GCHQ（Government Communications Head Quarters）などの SIGINT（SIGnal INTelligence）機関は[117]、一般人の目に触れる活動を行うわけではないので、その存在すら秘匿した時代が長かった[118]。

しかし、情報公開による「開かれた政府」を求める声や、冷戦の終結による緊張の緩和などの流れの中で、インテリジェンス機関といえども国民の理解なしでは成り立たないことが意識されるようになっていった。そして現在では、インテリジェンス機関とサイバーセキュリティ対策は、切っても切れない関係になっている。前述の ISA 1994 や、その前の Security Service Act 1989 が「開かれた政府」の先例であり、そこで権限が明記された GCHQ の内部に、全英のサイバーセキュリティに責任を負う NCSC（National Cyber Security Centre）が設置されたことは、両者の関係を象徴する出来事である[119]。

6.3 2010 年代におけるにログの利活用に関する規律

わが国におけるログの扱いは、少なくとも「電気通信事業におけるサイバー攻撃への対処と通信の秘密に関するガイドライン（第3版）」（インターネットの安定的運用に関する協議会 [2014]）までは[120]、 a) 通信の内容が推知できる限りログの知得も「通信の秘密」に当たる、b) 障害復旧など最低限のログの保存は許されるが可及的速やかに消去すべきである、といった hands-off の原則論寄りに解釈するものであった。これは規制当局の意向もさることながら、事業者自身も謙抑的であった結果と評すべきであろう。

しかし、激変するサイバー空間の安全確保には、このような性善説的な発想では対応できない。2015 年（第 4 版）を経た 2018 年改定（第 5 版）の現行ガイドライン（インターネットの安定的運用に関する協議会 [2018]）でも、攻撃者の特定行為に関する Q&A で、「通信履歴（ログ）は通信の秘密として保護されるものであり、攻撃通信を行っている契約者を特定するため、自社の契約者の接続ログを解析し、当該契約者に連絡をすることは通信の秘密の侵害（窃用等）に当たりうる」として、従来の解釈を原則的には維持している（p.11）。

---

[116] 例えば、Park Jin Hyok に対する Criminal Complaint を参照。https://www.documentcloud.org/documents/4834226-2018-09-06-PARK-COMPLAINT-UNSEALED.html

[117] SIGINT は無線の傍受が中心であったが、今日では海底ケーブルからの傍受が中心になっており、その部分は COMINT（COMmunications INTelligence）と呼ばれることもある。

[118] NSA が No Such Agency の略号だとする笑い話は、人々の受け止め方を暗示している。

[119] NCSC は政府機関であるが、民間をも含めた全英のサイバーセキュリティを統括する組織であり、その仕組みに組み込まれた民間組織は、政府機関と同レベルのセキュリティ情報を共有することになる。

[120] このガイドラインは、当初「電気通信事業者における大量通信等への対処と通信の秘密に関するカイトライン」（第 1 版、2007 年）として制定され、その後第 2 版（2011 年）、第 3 版（2014 年）、第4版（2015 年）と改定されてきた。この間、策定団体の追加があったほか、タイトルも当初のものから、第 4 版以降は現在のものに改められ、サイバーセキュリティ攻撃対策の比重が高まっている。

しかしそれに続く後段において、「侵害の防止に他に有効な手段がない場合、攻撃を受けている受信者の設備等に生じる侵害を防止するため、必要かつ相当な範囲で契約者の接続ログの解析を行い、攻撃通信を行っている契約者を特定した上、これを止めるよう当該契約者に連絡をすることは、通常は、正当防衛又は緊急避難として違法性が阻却されると考えられる」としている。

ここでは未だ「正当業務行為として認められるべきである」とまでは言い切っていないが、ログも通信の秘密に含まれるとの理解を前提にしつつも、現実的な解釈を打ち出したもので、例外処理を明示した点で従来の枠を超えるものであると評価される。

他方で先進諸国は、世紀の変わり目辺りからサイバーセキュリティに、強い関心を持ち続けていた。特に EU は「サイバー犯罪条約」の制定を提唱し [121]、2001 年には実現にこぎつけた。わが国は条文のうち共謀罪の制定に反対意見が多く、加盟条件のクリアに 10 年近い時間がかかったが、2011 年に改正された刑事訴訟法 197 条には、表 13. のように第 3 項以下の規定が追加され、遅ればせながら法的レベルでログの利活用に道を開くようになった [122]。

表 13. 刑事訴訟法 197 条におけるログの保全要請

1 捜査については、その目的を達するため必要な取調をすることができる。但し、強制の処分は、この法律に特別の定のある場合でなければ、これをすることができない。
2 捜査については、公務所又は公私の団体に照会して必要な事項の報告を求めることができる。
3 検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、30 日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付差押えをする必要がないと認めるに至つたときは、当該求めを取り消さなければならない。
4 前項の規定により消去しないよう求める期間については、特に必要があるときは、30 日を超えない範囲内で延長することができる。ただし、消去しないよう求める期間は、通じて 60 日を超えることができない。
5 第 2 項又は第 3 項の規定による求めを行う場合において、必要があるときは、みだりにこれ

[121] サイバー犯罪に関する条約（略称、サイバー犯罪条約）は欧州評議会が主導し，2001 年にブタペストで署名されたためブタペスト条約とも呼ばれる、サイバー犯罪に関する国際的レベル合わせ（犯罪の類型化と手続きの統一の両面）を図った多国間条約で、現在 32 か国が加盟している（ロシア・中国は加盟していない）。わが国は、2011 年の刑法・刑事訴訟法等の改正を受けて、2012 年に効力発生。

[122] 正式には「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律」（2011 年 6 月 24 日法律第 74 号）による改正。

らに関する事項を漏らさないよう求めることができる。

もっともこの規定は、通信履歴を保存することを求めるものではなく、事業者等が自主的に保存しているログに関して、保全を要請できることを定めたものである [123]。保全要請とは、プロバイダなどに対し、差押え等をするため必要があるときに、業務上実際に記録している通信履歴（通信の送信先、送信元、通信日時などであり、電子メールの本文等の通信内容は含まれない）のうち必要なものを特定した上で、一時的に消去しないよう求めるもので、保全要請の対象となるのは、要請があった時点においてプロバイダなどが業務上記録しているものに限られる。

なおここで注目されるのは、第3項において「電気通信を行うための設備を他人の通信の用に供する事業を営む者」に加えて、「自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者」もまた、保全要請の対象になっている点である。これは青少年インターネット環境整備法における「特定サーバー管理者の努力義務」（注 91 と表 12-1 の注を参照）とも合わせて、本稿における「適用除外電気通信事業」を「通信の秘密」の保護主体に含める発想（1.2 節と表 1. ）を、間接的に支持してくれるものではないかと考える。

6.4 ログの保存期間

ログの保存は利活用を前提にしたものなので、どの程度の期間保存すべきかは、利用目的との関連で議論されることになる。現時点で、保存期間の原則を制定法で定めたものはなく、電気通信事業者に関しては、ソフト・ローである前述のインターネットの安定的運用に関する協議会［2018］が根拠になる。

なお政府機関に関するものとしては、2011 年に内閣情報セキュリティセンター（当時）が実施した「平成 23 年度 政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書」（https://www.nisc.go.jp/inquiry/pdf/log_shutoku.pdf）における、「ログは1年間以上保存する」という推奨がある。

その根拠は、「過去の標的型攻撃事例から、攻撃事象の発見からさかのぼると攻撃の実施された時期はおおよそ1年以内であり、ログを1年間保存すれば、高い確率で攻撃の初期段階からのログを抽出することができるため」としている。しかし、その後 EU の Data Retention Directive における保存期間の 3 年が、EU 司法裁判所によって憲章違反とされたことなどもあって [124]、この推奨がなお有効であるか否かは、定かではない。

なお、より幅広く関連書事項を調査したのは、IPA（情報処理推進機構）の「企業における情

[123] 通信履歴の電磁的記録の保全要請に関するQ&A http://www.moj.go.jp/houan1/houan_houan24.html
[124] 2014 年 4 月に欧州司法裁判所（CJEU）は、EU データ保存指令（Directive 2016/24/EC of 15 March 2006）を EU 憲章違反で無効とする判決を下した。

報システムのログ管理に関する実態調査」(2016 年 6 月)であろう。そこには、表 14. のような総括表が掲載されており(https://www.ipa.go.jp/files/000052999.pdf)、刑事訴訟法の規定も、NISC の指針も含まれている。

表 14. ログ保存期間の目安

保存期間	法令・ガイドライン等
1 か月間	刑事訴訟法第 197 条3項：通信履歴の電磁的記録のうち必要なものを特定し、30 日を超えない期間を定めて、これを消去しないよう、書面で求めることができる*。
3 か月間	サイバー犯罪に関する条約 第 16 条2項：必要な期間(90 日を限度とする。)、当該コンピュータ・データの完全性を保全し及び維持することを当該者に義務付けるため、必要な立法その他の措置をとる。
1 年間	PCI DSS：監査証跡の履歴を少なくとも 1 年間保持する。少なくとも 3 か月はすぐに分析できる状態にしておく。NISC「平成 23 年度政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書」: 政府機関においてログは1年間以上保存。SANS「Successful SIEM and Log Management Strategies for Audit and Compliance」:1 年間のイベントを保持することができれば概ねコンプライアンス規制に適合する。
18 か月間	欧州連合(EU)のデータ保護法。
3 年間	不正アクセス禁止法違反の時効。脅迫罪の時効。
5 年間	内部統制関連文書、有価証券報告書とその付属文書の保存期間に合わせて。電子計算機損壊等業務妨害罪の時効。
7 年間	電子計算機使用詐欺罪の時効。詐欺罪の時効。窃盗罪の時効。
10 年間	「不当利得返還請求」等民法上の請求権期限、及び総勘定元帳の保管期限： 商法 36 条。(取引中・満期・解約等の記録も同じ扱い) 銀行の監視カメラ、取引伝票に適用している例あり。

*(引用者注)表 13. にある通り、保存期間ではなく保全要請の期間であり、特に必要があるときは最大 60 日まで延長できる。

なお、電気通信事業者が取得するログのうち、「接続認証ログ」に関しては、現行の「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」では [125]、以下のような複雑な構成になっている [126]。まず、本文では表 15. のように記述している。

[125] 2017 年4月 18 日総務省告示第 152 号。

[126] 2015 年改正時の同ガイドラインでは、保存が許容される期間について具体的に、「接続認証ログの保存については、事業者が正当業務の遂行に必要とする場合)、一般に6か月程度の保存は認められ、適正なネットワークの運営確保の観点から年間を通じての状況把握が必要な場合など、より長期の保存をする業務上の必要性がある場合には、1年程度保存することも許容されると考えられる」となっていた。

表 15. 総務省の個人情報保護ガイドラインにおけるログの扱い

（通信履歴） 第 32 条 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、当該電気通信の相手方その他の利用者の電気通信に係る情報であって当該電気通信の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。 2 電気通信事業者は、利用者の同意がある場合、裁判官の発付した令状に従う場合、正当防衛又は緊急避難に該当する場合その他の違法性阻却事由がある場合を除いては、通信履歴を他人に提供してはならない。

これを受けた、通信履歴の記録（第 32 条第 1 項関係）の解説では「保存期間については、提供するサービスの種類、課金方法等により電気通信事業者ごとに、また通信履歴の種類ごとに異なり得るが、業務の遂行上の必要性や保存を行った場合の影響等も勘案し、その趣旨を没却しないように限定的に設定すべきである」としつつ、電気通信事業者が取得するログのうち、「接続認証ログ」に関しては、表 16. のような注が追加されている。

表 16. 総務省の個人情報保護ガイドラインにおける接続認証ログに関する注記

例えば、通信履歴のうち、インターネット接続サービスにおける接続認証ログ（利用者を認証し、インターネット接続に必要となる IP アドレスを割り当てた記録）の保存については、利用者からの契約、利用状況等に関する問合せへの対応やセキュリティ対策への利用など業務上の必要性が高いと考えられる一方、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ことから、電気通信事業者がこれらの業務の遂行に必要とする場合、一般に6か月程度の保存は認められ、適正なネットワークの運営確保の観点から年間を通じての状況把握が必要な場合など、より長期の保存をする業務上の必要性がある場合には、1年程度保存することも許容される。

こうした複雑な構成は、前述の欧州司法裁判所の判決によりログの扱いが一時的な空白状態にあるための、やむを得ない措置かもしれない。事実、ログの保存期間に関する先進諸国の態度は、揺らぎの中にあるように見える。

EU が検討中の e プライバシー指令案では、狭義の電気通信事業者のみならず高度通信事業者（俗に Over-The-Top = OTT 事業者ともいう）をも規律の対象としているので、実行上市場を席巻する、いわゆる GAFA 等の巨大企業も電気通信事業者並みの扱いになる。これを先取りした仏国は、前述の「デジタル共和国法」において、GAFA への「通信の秘密」規定の適用を明記している [127]。

[127] ただし、仏国においても他の先進諸国におけると同様「通信の内容」と「ログ」の扱いはアンバンドルされているので、OTT に関する規定がどこまでログに適用されるのかは、未だ明らかではない。

これは片方で、規制当局がログの保存を当然視せざるを得ないことを意味するが、他方で巨大企業といえどもプライバシーへの配慮を欠いてはいられないことをも意味する。例えば石井［2020］で紹介されている、検討中の e プライバシー指令案において、事業者が「セキュリティに危険を及ぼす可能性のある具体的なリスクが存在する場合」に、「エンド・ユーザーに通知しなくてはならない」との規定は、ログの知得と分析なしではあり得ないので、前者の例である。逆に、Google がログの保存期間を 12 か月から 9 か月に短縮すると報じられていることは[128]、後者の例かと思われる。

6.5 ログの利活用の正当化理由

6.1 節で述べたように、ログの利活用は先進諸国では何らかの形で行われているが、「通信の秘密」が厳格に解釈・運用されてきたわが国の現状では、法改正等の提案以前に「なぜ」また「いかなる条件の下で」、例外措置が許されるべきかを論じなければならない。

ログの利活用の正当化理由は、本来なら違法性阻却事由の 1 つである「法令に基づく正当行為」あるいは「正当業務行為」に該当するか否かで判断されるべきであろう。しかし現実に該当する法令等がない場合は、一般的な違法性阻却事由である「正当防衛」あるいは「緊急避難」に該当するか否かで論じられてきた。これは「通信の秘密」侵害には刑事罰があるため、刑法の一般原則に沿った慎重な手続きといえよう[129]。

その内容は、一般的には ① 目的の正当性、② 行為の必要性、③ 手段の相当性、の 3 要素をすべて満たすものと考えられてきた[130]。① は当該行為の目的が正当なものであるか否かを、② は当該行為が目的達成に必要であるかどうかを、③ は各種の手段の中でも相当なものが選択されたか[131] などを、チェックするものである。

この 3 要件は、「法令に基づく」場合も、そうでない場合も共通と考えられるが、前者の方が法令審査の過程で妥当性が十分に検討され、要件が明文化されるので望ましい。しかし、サイバー・インシデントのように次々と新しい攻撃が生み出されるような場合には、法令で定めることは時間を要するから、「正当行為」であるか否かを判断する基準を、ソフト・ローに求める頻度は高くならざるを得ない。

現に、従来「違法性阻却事由あり」とされたケースは以下のようなものであり[132]、いずれもガイドライン（インターネットの安定的運用に関する協議会［2018］）に記述され、それに沿って実

[128] 例えば、https://xtech.nikkei.com/it/article/NEWS/20080910/314515/

[129] 刑法 35 条は「法令又は正当な業務による行為は、罰しない。」と、同 36 条 1 項は「急迫不正の侵害に対して、自己又は他人の権利を防衛するため、やむを得ずにした行為は、罰しない。」と、同 37 条 1 項本文は「自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。」と規定する。

[130] この判断基準は総務省の研究会が案出したもので、正当防衛と緊急避難では構成要件が異なるため、標準的な刑法の教科書では、より緻密な議論が展開されている（例えば、山口［2015］参照）。

[131] 民事の分野では、人権侵害の度合いが最も低いもの、言い換えれば LRA=Less Restrictive Alternative がないもの、といった概念に近いものと思われる。

[132] 読者に分かりやすいよう、私たち流に表現を若干修正している。

行されている。

a) 電気通信事業者が課金・料金請求の目的で、顧客の通信履歴を利用する行為、

b) ISP がパケットのヘッダ情報を用いてルートを制御する行為等、通信事業を維持・継続する上で必要な行為、

c) ネットワークの安定的運用に必要な措置であって、上記の 3 要件を満たす行為。

なお、このうち c)について上述の「サイバー攻撃対処と通信の秘密ガイドライン」は、本文で「大量通信に対する帯域制御」を例示し、注で OP25B、IP25B（TCP ポート 25 番への出力や入力をブロックすることでスパム・メール等を回避すること）を挙げている。しかし、ガイドラインの性格と法令に代替する効果が期待されていることからか、サイバーセキュリティ対策が一般的に「違法性が阻却される」とまでは言い切っていない。

これは現行法を前提にすれば、人権を重視した慎重な態度として賞賛すべきことかもしれない。しかし上記 a) や b) は凡そ電気通信事業を営む以上必要不可欠な行為であり、ことさらに「違法性が阻却される」という証明が求められる事案ではないと思われる。現に諸外国の通信キャリアから、このような議論があると聞いたことがない [133]。

それを比喩的に表現すれば、「外科医が手術をする行為は外形的には傷害罪等に当たり得るが、手術によるのが最も確実性の高い回復措置であるとして、患者の同意を得れば、違法性が阻却される」ことを改めて確認しているようなものであろう。違法性が阻却されるのは例外であり、例外は制限列挙すべきという主張も分からぬではないが、余りに厳格で現場の実感とはかけ離れた議論のように思われる。何らかの法令に、サイバーセキュリティ対策としてのログの利活用が、正当業務行為である旨を明記することが望まれる。

いずれにせよ、電気通信システムを含む自律システムにおいては、多種類かつ大量のログが記録される。これを長期間保存することはプライバシー侵害のリスクを高める一方、システムの安全を維持したり犯罪の証拠として利活用するためには、一定期間のログが保存されていることが望ましい。この両立しがたいバランスをどう取るかは難しい問題であるが、最適化に成功した国が国際的な信用と競争力を獲得できることも、また事実であろう。

概していえば、わが国の現状はリスク回避の極端に位置していると思われるので、折角のログ情報が「宝の持ち腐れ」になっているだけでなく、「国際競争力の低下」さえ招いているのではないかと懸念される [134]。先進諸国の有力な電気通信事業者や情報処理業者は、ログの分析から得たデータを利活用して、顧客システムのモニタリングやセキュリティ対策を契約ベースで提供する MSSP（Managed Security Service Provider）になって [135]、顧客を囲い込むに熱心である。こうしたトレンドに遅れることのないよう、セキュリティ産業育成の視点も忘れてはならない [136]。

---

[133] a) は複数の事業者が存在すれば料金精算のために不可欠な作業であり、b) はパケット通信なら大前提となる行為である。

[134] 多数のリスクを克服して観光客のホワイト・ハウス見学さえ認める国と、リスクを恐れるあまり文化的価値の高い施設も限定的にしか公開しない国の、メンタリティの差と言うべきだろうか。

[135] この場合には、約款あるいは個別の契約でログの利活用に関し利用者の同意を取ることになるので、違法性がないことは、より明確になる。

[136] 2020 年 7 月に公表された「IoT・5G セキュリティ総合対策 2020」においては、「国産のセキュリティ・ソフトが弱いので、データ

6.7「通信の秘密」の普遍的価値

ところで、これまでの記述では、従来の「通信の秘密」の背景にある原則がすでに変質している点や、厳格な解釈が実務上の桎梏となっている点に重きを置いて説明してきたが、これをもって共著者が「通信の秘密」を軽視していると誤解しないでいただきたい。

通信ビジネスに長年従事してきた共著者には、「通信の秘密」が持つ価値は、骨の髄まで浸透している。そして現実の世界でも、「通信の秘密」の価値が再評価される例が生じている。その具体例は、2019 年 1 月 23 日付の EU 委員会の日本に関する「個人情報保護に関する十分性決定」において、大きな理由として「通信の秘密」の規定に言及していることである [137]。

また学界においても、宍戸常寿は「表現と人権が守られ、誰もが安全に安心して利用できることが、インターネットの自由の柱です。（中略）表現の自由やプライバシーの基盤がそれほど強くない日本では、憲法の『通信の秘密』規定が数少ない土台になってきた経緯があります」と述べ、個人データ保護における「通信の秘密」の規定の重要性を指摘している [138]。

成原［2018b］も「通信の秘密が仕える価値の普遍性」を強調し、「通信の秘密が憲法上明文で保障されていない米国でも、通信の秘密と重なり合う価値（表現の自由、プライバシー、サイバーセキュリティ）は尊重」されていると指摘している。「通信の秘密は、わが国特有の『ガラパゴスなルール』などではなく、それが仕える価値は普遍的」であって、欧米の近年の議論（プライバシーと表現の自由の相互依存性、メタデータの収集・分析によるプライバシー侵害のリスクへの着目）を踏まえると、「わが国の通信の保護の在り方は再評価されるべき側面があるのではないか」と述べている。

この両者に共通するのは、法制度こそ違うが「通信の秘密」の保護法益は欧米各国と共通点があり、「通信の秘密」を表現の自由やプライバシー保護の法制度と併せて一体として捉えるべきとの視点であると考えられる。すなわち、法的な用語は異なるものの、「通信の秘密」は欧米と共通する普遍的価値を目指していると考えられるので、インターネット利用において「通信の秘密」の保護を制限する事例が多くなったとはいえ、その原則を堅持することには十分な理由があるといえよう（林・田川［2019］）。

従って、「通信の秘密」の問題をプライバシー・個人情報保護、さらには実効性のあるサイバーセキュリティ法制の整備と一体として検討することが、欧米の法制度との普遍的価値の共有につながり、サイバーセキュリティに関する国際連携や法研究における国際的なハーモナイゼーションを強化することに寄与すると考えられる。

負けしてしまっている」、「攻撃者との戦いはもとより、先進国との競争にも勝てない」という指摘がある。注 87 も参照。

[137] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0419c 。十分性決定に関する EU との交渉経過については、同文書の前文（116）、（129）と、堀部［2019a］［2019b］を参照。

[138] 朝日新聞デジタル 2018 年 9 月 7 日「（耕論）サイト遮断と言うけど 赤松健さん，宍戸常寿さ ん，別所直哉さん」

6.8 スノーデン文書から推測するインテリジェンス機関におけるログの利活用

本節は他の節と違い、スノーデン文書を日本語で解説した茂田忠良の労作（警察政策学会[2015]）を足掛かりに、インテリジェンス機関におけるログの利活用を推測するものである [139]。情報共有の第 5 段階におけるあるべき施策を論ずることで自制し、第 6 段階の施策を将来の課題としている本稿では、異質の節となる。

なぜ本節を設けたかと言えば、以下の理由でわが国が先進諸国の間で孤立しているため、如何に第 5 段階から脱却して第 6 段階へ移行できるかを視野に入れた提言を行うことが、不可欠だからである。

a) 電気通信事業者は「通信の秘密」に関する通説的理解に従順であるため、サイバー対策においても、通信ログの分析は自粛していると推測される、
b) 電気通信事業法適用除外事業者は、業務上の必要があれば通信ログを含むログの分析を行っていると推測されるが、電気通信事業者に準じて扱いに慎重を期しており、その内容を公開していない、
c) わが国には先進諸国と匹敵し得る SIGINT 機関が存在しないので、インシデント情報の収集は民間企業、特に電気通信事業者に依存せざるを得ない。

警察政策学会 [2015]によれば、インテリジェンス情報の収集には次の 8 つの経路があるという。① 民間企業のデータ・センターから、② 電気通信の基幹回線から、③ 外国通信衛星の傍受による、④ 外国にある公館における特別収集サービス（Special Collection Service）から、⑤ CNE（Computer Network Exploitation）による、⑥ セカンド・パーティ、サード・パーティの協力国から、⑦ SIGINT 衛星と機上収集による、⑧ 従来型収集（conventional）による。

これらが全体の情報量のうちどの程度を占めるかは不明であるが、本稿の目的からすれば、ログに相当する情報の比率さえ推定できれば十分であろう。すると、記述の頻度と分量や報道された後の世論の反応などから、① の代表例である PRISM と、② による主要キャリアの基幹回線からの知得が、特に重要であることが読み取れる。

前者の PRISM 計画は、マイクロソフト、Yahoo、Google、Facebook、PalTalk、YouTube、Skype、AOL、Apple の、合計 9 社のウェブ・サービスを対象に、ユーザの電子メールや文書、写真、利用記録、通話など、多岐に渡るメタ情報の収集プログラムであり、「NSA の Crown Jewel」と呼ばれている。一方、後者は約 20 の計画により世界のインターネットの主要ポイントにおいて、膨大なデータを収集するものである。「米国の内と外、収集の法的根拠、民間企業の協力の有無、米国外の場合に他国の諜報機関の関与の有無、具体的な取得データの中身など、様々なものが含まれており、一様ではない」とされる（警察政策学会 [2015]）。

いずれも（少なくとも米国においては）民間企業の協力を得て行う SSO（Special Source Operation）であり、バルクデータとして取得後、「XKeyscore というデータベースに一定期間記

[139] Snowden の暴露から既に 7 年以上が経過しているので、当時の分析は out-of-date になっているかもしれない。特に、「生き馬の目を抜く」インテリジェンスの世界では、「対象に知られたら方法を変える」のが原則でもあるので、意図的な変更もあり得る点に注意が必要である。

録され、更に情報価値があると判断されるデータは、別のデータベースにも長期間保管される構造となっている」（警察政策学会［2015］）。

ここで注目すべきは、以下の 3 点かと思われる。

a) サイバーセキュリティ対策においては、関連情報の収集が第一歩であり、その点でインテリジェンス活動と親和性を持っている、

b) その中では、情報サービスに関するログと通信ログとが、最も重視されている、

c) 世界最大の SIGINT 機関といえども、これらの情報収集を全部自前で実行するのは難しく、主要な民間企業の力を借りている。

上記の 3 点を言い換えれば、表 6. における情報共有の第 6 段階を目指すのであれば、第 5 段階にある状況においても、その備えを念頭においておかねばならない、という教訓であろう。第 6 段階は本稿の射程を超えるが、それへの移行を常に念頭に置きつつ検討することが求められる。

第3部　自律システム管理責任の明確化と対象を特定した通信ログの利活用

7　わが国法制の要改善点

7.1 自律システム管理責任と留意事項

第 2 部までの分析、とりわけ先進諸国の法制度との比較から得られた教訓は、一言でいえば「自律システム管理責任」の明確化ということになる。それを分節化すれば、1) 起点ともいうべき「ネットワーク・システムのモニタリング」と、2) モニタリングから得たログ情報を自らが所有するシステムのサイバーセキュリティ対策に利用することの正当化と、3）モニタリング等から得たインシデント情報を所管官庁に届けることの義務付け、4) 当該情報を他者と共有しサイバーセキュリティ対策として活用することの正当化、の 4 段階になると思われるので、これらを中心に以下の各節で簡潔にまとめておこう[140]。

その際、3.5 節～3.7 節で述べた基本理念は、時代が変わっても修正する必要はないと思わ

[140] なお 1)～4)の責任のうち、重要社会基盤事業者に課されるのは、3) のみである。また第 2 部と違い第 3 部では、通信ログだけでなくログ全般に関して論ずる。この意味で第 2 部は、「通信の秘密」の保護下にある通信ログに限定した分析であると理解していただきたい。

れる。しかし、先進諸国とわが国との環境の差を踏まえて、個別具体的な規定の仕方に関しては、強調しておきたい点が少なくとも 4 点ある。

第 1 点は、自律システム管理責任を負う者を幅広く捉えるべきことである。現在のネットワークは「自律システム間の相互接続」へと変化しており、電気通信事業者に期待された機能を、自律システムの所有者（あるいは運営者。電気通信事業者とともに、サイバーセキュリティ基本法の定める「サイバー関連事業者」の中心を占める）にも広く期待すべき環境になったからである[141]。

第 2 点は、自己責任を果たすために、制定法に権限と責任を明記すべきことである。インターネットは「自律・分散・協調」を理念としており、自己責任（場合によっては自力救済を含む）を求められることが多い（林・田川 [2018]）。制定法主義を採るわが国においては、法律に根拠を置くのでなければ規範力が弱くなってしまうので、サイバー関連事業者全体に関して何らかの形での「法的権限と責任の明示」が必要ではないかと思われる[142]。特に「自力救済の禁止」は制定法主義の下では大前提とされるので、米国の PE（Provider Exception）に相当する正当化根拠は不可欠であろう。

第 3 点は、本稿におけるログの利活用の提案は、悉皆的（バルク型）モニタリングで得た情報がすべて利活用可能であることと同義ではないことである。前述の通り本稿では、「ログのバルク知得を認めるが、不審なログに早期に絞り込んだ上で残りは消去し、特定データの形でしか利活用を認めない」とする立場（知得におけるバルクの容認と、利活用におけるバルクの否定。これは 1.3 節のおける「ログの利活用に関する 9 原則」を言い換えたものである）を採るつもりである。

第 4 点は若干法技術的な問題で、「法と技術の調和」が求められることである。わが国の法制は「設備」とその「技術的要件」を中心に規定されており、「制度を技術で担保する」仕組みになっている。これは、技術に多くを依存する電気通信の世界を律する方法として有効である反面、「法と技術」という学際的な相互理解を必須とする側面も内包している[143]。「法と技術」に関する経験はわが国では乏しいので、特に法学者が難しい技術問題を敬遠して技術者に「丸投げ」せず、正しい意味での「リーガル・マインド」を育てるためにも、制定法に根拠を置くことが期待される。

7.2 起点としてのモニタリング

米国が、サイバーセキュリティ情報共有法において「民間企業が自身の情報ネットワーク・シ

---

[141] 現在のインターネットの先駆けとなった「電気通信とコンピュータの融合」や、「通信と放送の融合」という現象は、これらの融合分野を律する共通原則を必要としている（林 [1984] [2005a]）が、4.2 節で述べたように、整合が取れたものにはなっていない。注 86 を参照。

[142] 法律で定めることは必要条件だが十分条件ではないので、直ちに実効性が担保されるわけでもない。注 38 を参照。

[143] 米国では Law & Technology は広く受け入れられた研究アプローチであり、主だったロー・スクールではその名を関するジャーナルを発行しているのが普通である。しかしわが国では、『L&T』という市販雑誌があるのみで、学際的研究として十分発展していない。

ステムはもとより、委託を受けた場合は他者のものであっても、これをモニタリングすることができる」と明文で認めたことは、サイバー空間のセキュリティ確保の起点となり得るものである。わが国では「通信の秘密」の厳格解釈のため、少なくとも電気通信システムに関する限りモニタリング自体が自粛されている（萎縮効果）と思われるので、それを解き放ちグローバルなコモン・キャリアと競い合うMSSPを育てるためにも必要であろう。

もっとも米国は「民間主導」を第一義とする国なので、これを法的な義務とはせず、免責の根拠とするにとどめている。しかし米国は防衛装備品の調達の際には、セキュリティ確保についての厳格な規格の順守を求めるほか、セキュリティ・クリアランスについても同様なので、いわばミリタリー・スペックが範となって、民間企業のセキュリティ手順のレベルが上がっていく仕組みを採っている。免責による民間企業の自主的な行動を促せば、十分な効果があると見ているのであろう（永野［2020］）。

とすると、軍事主導があり得ないわが国の場合、EUのように後述する（7.4節）インシデント情報の報告義務を重視した方が、「手っ取り早い」かもしれない。しかし、安全保障で緊密な関係にある米国と違った仕組みを採ることには、リスクが高すぎる（米国の防衛装備品の入札に参加するには米国流のリスク管理と認証取得が求められる[144]、GSOMIA＝General Security of Military Information Agreementでも情報保全について同じレベルが求められるなど）。そこで、基本的には米国流に合わせ、EU 方式に良さがあれば補完するといった、ハイブリッドの仕組みがベターではないかと思われる。

さて、このように米国から教訓をくみ取ったとして、それをわが国で十分に生かすことは可能だろうか。実は米国的発想は、a) サイバーセキュリティとログが密接な関係を有していること（1.1節）、b) store-and-forwardのインターネットではログの役割が桁違いに大きくなること（2.1節）、c) コンテンツに関する間接責任と自律システム管理責任とは分けて考えるべきこと（5.2節）、d) 自律システム（AS）内は AS 所有者の自律的管理に委ねるべきこと、などの認識が共有されているからこそ、生まれたものであろう。

しかし、わが国にも同様の指摘をした先駆者として多賀谷一照がおり、音声電話では電気通信事業者以外の第三者が「通信の秘密」を侵す可能性は低いが，データ通信（今日的にはインターネット[145]）においては，その可能性が高まったので、現在の「通信の秘密」の概念を見直すべきとの主張を早くから行ってきた（多賀谷［1995］）。

彼によれば、「通信の秘密」の主観性・形式性が人格権的な保護の法理に近い外形をもっているのは、音声通信の技術的特徴・制約に負うところが多いからに過ぎない（林・田川［2018］）[146]。このような議論の蓄積が既にあり、現にサイバーセキュリティ対策に関する通信ロ

---

[144] 2.4節で述べたように、わが国では民間企業向けのISMS（Information Security Management System）の認証取得で十分とされているが、米国では防衛装備品の調達に参加するためには、より高度なCMMC（Cybersecurity Maturity Model Certification）が求められる（永野［2020］）。

[145] データ通信という用語が使われているのは、インターネットが広く普及する以前の 1995 年に著されたためであろう。

[146] 多賀谷は、新しい発想として以下の4点を強調している。① 基本的セキュリティの確保：システムとしての通信の秘密総体，通信が安全かつ確実になされることを保障。 ② 狭義の「通信の秘密」：通信のすべてではなく、人と人との間の私的な 1 対 1 の通話の実質をもつものに限定して維持。③ 他の法益による通信内容の保障：上記以外の通信も、プライバシー保護・営業秘

グの扱いに関して弾力的な規定を設けていることから（6.2 節～6.3 節）、日米の差は表面的なもので、実質的な受け入れの素地はあるものと思われる。

また、わが国の事業法における設備関係の規律をよく読めば、「設備」とその「技術的要件」を中心に構成されているようでいて（4.1 節）、その背景には自律的管理によるモニタリングなどを受け入れる余地は残されている、とも言えそうである。

ただし、わが国では現在情報処理と電気通信の主務官庁が別々になっていることや、サイバーセキュリティに関する司令塔が内閣官房サイバーセキュリティセンターであり、調整機関に過ぎないのではないかとの懸念がある。前者は 1970 年代から 80 年代前半にかけての「VAN 論争」以来の懸案であり、後者は既に「サイバーセキュリティ庁を設置すべし」とする提言も出されている（笹川平和財団 [2018]）。これらの課題に対しても、並行して対応する必要があることを、付言しておきたい [147]。

7.3 ログの自己利用の正当化

先進諸国から学ぶべき第 2 点は、モニタリングから得たログ情報を、サイバーセキュリティ対策 [148]として自己利用することの正当化である。そのためには正当な利活用の「適正手続」と「免責」の明示が必要になる。この点に関しては、ネットワークを介して運ばれる情報（コンテンツ）に関する ISP の責任に関する考え方と分類が参考になる。

前述の通り米国では、直接責任を原則としながらも、一定の条件下では間接責任を問うことを躊躇しないやり方はもとより、ケースを分節化（アンバンドル）して、サイバーセキュリティには間接責任が不可避である点を指摘している点で、他の諸国より進んでいるように思われる [149]。そこで、前節のモニタリングの権限規定を設ける場合には、同時にそこで得たログ情報をサイバー対策として自己利用することができる旨を為念的に記しておくことが望ましい。

そのような対象企業の範囲を定める概念として、サイバーセキュリティ基本法には、a) 重要社会基盤事業者（同法 6 条）、b) サイバー関連事業者（同 7 条）、c）サイバーセキュリティ協議会の構成員（同 17 条）の 3 つの候補者がある。

密の保護・消費者の保護など、他の法益の観点から保護の対象となる。④ 「通信の秘密」のソフト的な捉え方：21 世紀においては、通信内容の保護・セキュリティ保護の重点は、回線のセキュリティから暗号鍵の保護に移っているはず。

147 そして何よりも、かつては「ジャパン・アズ・NO.1」とまでいわれた国が、なお「失われた 30 年」から脱却できないこと、その主な原因がシステム的思考の欠如にあることを（林 [1998b]）、深刻に受け止めるべきであろう。今般のコロナ対策における特定定額給付金の遅れがその象徴である。サイバーセキュリティはそれ自体で売り上げを伸ばす面は弱いが、「実空間でもサイバー空間でも世界一安全な国」との評価を勝ち取ることができれば、デジタル・トランスフォーメーションの過程で追いつくことができるかもしれない。そのような意味で、菅首相が掲げる「官庁の枠を超えた取り組み」が望まれる。

148 対策は防御に関するものであって攻撃を含まないことは、既に述べた（5.2 節の表 10.）が、ここで再度注意を喚起しておきたい。

149 ちなみに Wikipedia の Online Service Provider（OSP）Law の項目は、専ら Liability について記述されており、しかも米国の欄が a) 名誉毀損、b) 著作権以外の知的財産権侵害、c) 著作権侵害、d) セキュリティ、の 4 項目に分類されているのが注目される。4 分類は米国だけで他の諸国は 2 分類が多いこと、セキュリティを挙げているのが米国だけであることが印象的である。上記の 4 分類のうち、b) の記述はごく少量なので c) と統合し、ア)「検閲の禁止」が最も強く期待されるべき情報、イ)知的財産等として排他権が付与されている情報、ウ)インターネットの接続に不可欠でその安定的提供に有用な情報、として日本的に再構成することも、漫画村事件の教訓を生かす意味では有益かもしれない。5.3 節も参照。

この 3 者を比較すると、a) の重要社会基盤事業者は 14 業種に限定されて狭すぎ、c) サイバーセキュリティ協議会の構成員は自由意思で参加するので意欲は高いが、これまた現時点では狭すぎるし、未だ成果が判明する段階ではない。とすると、3.5 節の表 7. で概念が不明確の欠点があると指摘したものの、逆にその広汎性を生かして、b) のサイバー関連事業者に広く認めておくのが現実的かと思われる。

なお、ログの自己利用が認められる事業者には、個人情報保護法に準じて適正な手順を定め、責任者の常置を義務化することが有効ではないかと思われる。責任と免責を論ずるためには、そのプロセスを明確にし、責任者を特定する必要があるからである。このような諸点を総合すれば、前節の記述は米国的でもなんでもなく、わが国にも適用可能だし、適用する価値は十分あるものと考えられる。

7.4 インシデント情報の所管官庁への報告

インシデントとは、一般的には「出来事、事件、事故、事案、事象、事例などの意味を持つ英単語」であるが、「情報セキュリティの分野では、情報管理やシステム運用に関して保安上の脅威となる事象のことを指し、セキュリティ・インシデントとも呼ばれる。ウィルス感染や不正アクセス、アカウント乗っ取り、Web サイト改竄、情報漏洩、迷惑メール送信、サービス拒否攻撃（DoS 攻撃）などが含まれる」（IT 用語辞典 eWords）とされている。

わが国でも使われる脅威情報、米国の CISA of 2015 でいう CTI（Cyber Threat Indicator）は、インシデント情報とほぼ同じものと考えて良いだろう [150]。また仏国において「利用者の同意なしに通信の秘密に属する情報が利用可能な場合」である、「通信の表示・分類・ルーティングのため、または迷惑メールやマルウェアの検出のために、自動処理により分析する」（3.4 節）結果得られる情報も、インシデント情報に近い概念と思われる [151]。しかし、より法律的な定義としては、EU 指令におけるリスクの定義を基礎に「NIS（Network and Information System）に悪影響を及ぼす可能性があると合理的に特定可能な状況又は事象」に関する重大な情報とするのが、ベターかと思われる。

ネットワークのモニタリングを行えば、インシデント情報や、直ちにインシデントと断定できないがその疑いが濃い情報が入手できる。これを自己のシステムの防御用に用いることは前節で述べたとおり認められるが、所管官庁に届け出ることによって同業他社の参考に供することは、感染症対策として発症状況を当局に届け出ることと似ている。残念ながらサイバーセキュリティの現状は攻撃者が比較優位にあり、この状況は当面継続すると思われるので、防御側が備えを強化するには、この報告制度は有益である。

---

[150] インシデント情報は組織の長などに報告して理解を得るため、ログ情報という機械処理に向いたデータそのものではなく、narrative 的な加工を施したものである場合が多い。なお別にデジタル・フォレンジックの分野では IoC（Indicator of Compromise）という語も使われるが、その場合は証拠あるいは証跡としての採用が暗黙の前提になっているように思われる。本稿では、この中間程度の粒度あるいは加工度の情報を想定している。

[151] 人手が介在せず、一貫してコンピュータ処理によることが前提とされている。1.4 節で述べた「syntactic 的利用」という分類を思い出していただきたい。

特に EU において報告制度が重視されており、その状況は 3.3 節で詳しく紹介したとおりである。なぜ EU が報告制度に重きをおくかといえば、米国のような調達手続きを通じた強制の仕組みも、GAFA のような強力な IT 企業もなく、加えて加盟国が 28 か国（英国を含む）と多い EU 諸国では、政府主導での事故情報報告の一元化と SPC の設置を必要としている、と読めなくもない。

これに対して、わが国の報告制度は産業によってかなりの幅がある。最も厳格な例は総務省関連で、電気通信・放送・有線放送の 3 事業とも、重大な事故は即座に、その他の事故は四半期単位で報告が義務付けられている [152]。他の重要インフラ分野でも、報告義務・立入検査・改善命令などの制度は整っているが、それらの基礎となる保安規定や技術基準についての整備状況は複雑で、実際の運用までは比較できない [153]。何もかも一律の規制が望ましいわけではないが、セキュリティの盲点の 1 つが weakest point にあることに鑑みて [154]、全体を底上げする方法で、統一的な報告を義務付ける方向に展開していくことが望まれる。

ここで、1 点だけ予めお断りしておきたいのは、モニタリングの権限と責任はサイバー関係事業者を対象にし、インシデント報告義務は重要社会基盤事業者を対象にするとして、両者の扱いを分けている点である。これは、統一したセキュリティ対策を追及する上でマイナスとなることは避けられないが、表 6. における情報共有の第 6 段階に到達するまでの過渡期的な対応として受け止めて欲しい。サイバー事案に最も近い位置にあるのが前者であるから、後者の実力が向上した頃合いを見て、次のステップを検討することになろう。

7.5 インシデント情報の共有

インシデント情報を所管官庁に報告することは、同業他社の利活用を促進するが、民間企業としては、サプライチェーンを構成する関連会社との共有の方に、より強い関心があるかもしれない。攻撃者はサプライチェーンをターゲットにしているし、企業側もグループ経営を志向している場合が多いからである。また、サプライチェーンの 1 か所の脆弱性が上述の weakest point になり、全体のセキュリティ・レベルを落としてしまうからである。

その意味では3.7節で紹介したサイバーセキュリティ協議会を通じた情報共有は、従来の方法から大きく前進するものであり、サイバーセキュリティ基本法に根拠を持つものなので、なおさら期待が高まる。しかし、企業の反応はそうしたレベルにはないようである。表 17. は、NISC 資料として正直に公開されている参加希望企業との FAQ であるが、ここで懸念が表明されているのは、主としてサイバーセキュリティ基本法 17 条 3 項にある「協議会は、（中略）その構成員に対し、サイバーセキュリティに関する施策の推進に関し必要な資料の提出、意見の開陳、

[152] 電気通信事業に関しては、注 70 に同じ。
[153] 重要インフラ 14 分野の比較表（2019 年 4 月時点）は、以下を参照。
https://www.nisc.go.jp/conference/cs/ciip/dai18/pdf/18shiryou02.pdf
[154] セキュリティ対策として best shot（トップ・ガンの超人的努力）、total effort（全員参加による努力の集積）、weakest point（脆弱性が最も高い分野を守る）の 3 つが不可欠だとする見方（Varian [2004]）。

説明その他の協力を求めることができる。この場合において、当該構成員は、正当な理由がある場合を除き、その求めに応じなければならない。」との規定に関するものであろう。

表 17. 構成員希望者の不安と規約における対処策

項目	事業者等の皆様が持ちうる懸念や不安	運用ルール（規約等）における措置
相談・情報提供の範囲	任意の相談・情報提供は、信頼する相手にしか見せたくない	情報提供者は、情報の共有範囲を設定可。当該共有範囲は、勝手に変更されない
監督官庁との関係	任意の相談をしたせいで、監督官庁等に処分されてしまうおそれはないか	情報提供者は、監督官庁等を情報の共有範囲から除外可
情報提供義務	情報提供義務が適用され、情報を何でも吸い上げられることにならないか	情報提供義務の発動要件を「大規模なサイバー攻撃」等に明文で限定
規約改正による義務の拡大	あとで規約が改正されて、情報を何でも吸い上げられることにならないか	規約の改正は、総会（民間企業等を含む全構成員で構成）における多数決で決定
入退会の自由	協議会に一度入ったら、 もう脱会できなくなるのか	届出により、いつでも協議会を脱退可

これを読むと情報共有の第一歩から企業の逡巡が感じられ、3.7 節で述べた基本認識との差が心配になる。しかし他方で、一般社団法人 JPCERT/ CC が政令指定法人として、協議会の連絡調整事務を担当することとなっており、これまでの経験も生かせるようになっているので、時間の経過とともに相互信頼が醸成されていくことに期待したい。

なお、サイバーセキュリティ協議会の構成員に特有の義務として規定されている守秘義務（17 条 4 項）と罰則（同 38 条）は、ログの自己利用とインシデント情報の所管官庁への報告、通信ログの他者との共有を通じて、すべてに適用されるべき準則ではないかと思われるので、サイバー関連事業者が共有する情報にも適用を拡大しておく必要があろう。

7.6 サイバー攻撃者に対する利用拒否

以上のほか、電気通信事業法 6 条の「利用の公平」規定の例外として、① 不正アクセス行為や不正指令電磁的記録の送信行為等の実行者等に対して、電気通信役務の提供を拒否することができる旨の明確化、②上記行為によって刑事罰に処せられた者または刑の執行を終えて一定期間を経過していない者に対して、電気通信役務の供給を拒否できることを明記

すること、などが期待される。この点は既存の論文で主張したことではあるが（林・田川［2018］、林・田川［2019］）、本稿における提言と同時に実施していただきたい。

7.7 要改善点のまとめ

以上をまとめると、この際検討すべき現行法の要改善点は、表 18. のようになる。

表 18. 現行法の要改善点のまとめ

提案の目的	具体的要改善点	提案の主根拠
1. 自律システムは所有者等が自身で守るという意識改革と手続きの具体化	1-1.自律システム所有者等に、自らの管理下にある情報システムはもとより、文書による委託を受けた他者のものを含めて、サイバーセキュリティ確保のために、当該システムを適時モニターする権限と責任を与えること。 1-2.上記の者は、通信ログとそこから派生する情報の守秘義務を負うとともに、管理責任者を常置し、適正な運用手順を遵守しなければならないこと。	米国サイバーセキュリティ情報共有法。手続きについては、EU の NIS Security Directive
2. サイバーセキュリティ対策において通信ログを自己利用し、より高度の対策が実施できるための手続きの具体化	2-1. サイバーセキュリティ対策としての要件を満たす場合には、通信ログをバルクで知得し、特定データに絞り込んだうえで、自律システムの安全性を確保するために、利活用できる手続きを定めること。 2-2. ログ情報が定められた手続きを超えて若しくは手続きに背いて知得され、又は窃用・漏示された場合には、守秘義務違反の罪に問われること。	林・田川［2019］および本稿
3. インシデント情報を所管官庁に報告するための手続きの具体化	3-1. インシデント報告は、業法毎に規定されており精疎様々であるため、徐々に重要社会基盤事業者間の平準化を図ること。 3-2. インシデント情報が定められた手続きを超えて、あるいは手続きに背いて知得され、あるいは窃用・漏示された場合には、守秘義務違反の罪に問われること。	本稿
4. インシデント情報をサイバーセキュリティ対	4-1. 共有が促進されるように、ソフト・ローを整備すること。	本稿。ただしハード・ローは形

策に生かす限りで、他者と共有することを可能にする根拠と手続き	4-2. インシデント情報が定められた手続きを超えて、あるいは手続きに背いて知得され、あるいは窃用・漏示された場合には、守秘義務違反の罪に問われること。	式的には整備済みであり、ソフト・ローが主眼
5. サイバー攻撃者への利用拒否（「利用の公平」の例外規定）	電気通信事業法 6 条の「利用の公平」規定の例外として、① 不正アクセス行為や不正指令電磁的記録の送信行為等の実行者等に対して、電気通信役務の提供を拒否することができる旨の明確化、②上記行為によって刑事罰に処せられた者または刑の執行を終えて一定期間を経過していない者に対して、電気通信役務の供給を拒否できることを明記すること。	林・田川 [2018]、林・田川 [2019]

なおここには、本来なら表に入れるにふさわしい改善提案であっても、本稿のテーマに直接関連しないかぎり、除外したことをお許し願いたい。その代表例は、「不正アクセス禁止法」と「プロバイダ責任（制限）法」の改正であろう。例えば、公益達成のために政府機関が行う行為が、不正アクセス禁止法などに触れて実施できないとすれば、表 6. における第 6 段階への移行そのものが不可能になってしまうので、その改善に向けた関係諸官庁の努力が必要なことを強調しておきたい（林・田川 [2018]）。

更に理論的には、2011 年に刑法に「ウィルス作成罪」が新設され [155]、2019 年には電気通信事業法に「対電気通信設備サイバー攻撃」の概念が導入されたが [156]、前者は検挙件数などから見ても、その手続きが万全であるとは言い難いように思われ、後者は事後的にインシデント情報を共有する方策を講ずるのみで、それを抑止する対策はもともと考えられていない。これらの対策も、時宜を得て検討されることを期待している。

8 具体的提言と若干の留保

8.1 ハード・ローとソフト・ロー、実体法と手続法

前章で検討した「要改善点」を具体化するには、制定法という「ハード・ロー」に拠るか、ガイドラインや標準手続きなどの「ソフト・ロー」に拠るかの選択肢がある。大陸法系のわが国においては、国家が強制力を有する制定法がデファクト標準であり、法解釈（特に裁判官の判断基

[155] 不正指令電磁的記録に関する罪、刑法 168 条の2、168 条の3。
[156] 2019 年の電気通信事業法等の改正による。

準）においても重視されてきた。この伝統は十分尊重に値するから、法的安定性の観点からは、できるだけ法律で規定することが望ましい。

しかし、インターネットの世界はドッグ・イヤーという言葉に象徴されるように、変化が激しい技術革新を前提にしているから、「法的安定性」が時に「法的硬直性」に転じかねない危険もある。そこで技術の世界では、標準的な手続きをマニュアルのような形で定め、随時改定していくことが常態化しており、法もこれに倣って、ガイドラインなど強制力は乏しいが弾力的運用が可能な方法が好まれる場合もある。このような自律型は、インターネットの発想にもマッチしている[157]。

また、同じ「要改善点」の目的を達成しようとする場合に、実体法的な規定を置くのが良いか、手続法を充実すべきか、という選択肢もある。従来は、法の中心は実体法であるとの固定観念があったが、インターネットの世界は「情報」という目に見えないものを相手にしているので、「手続きこそ実体を保障する」という面がある（林 [2017a]）。そこで、実効性の観点から見て、実体法的規定と手続法的規定、あるいはその組合せを選択することになる。本稿が、手続としてのログ（のうちでも特に通信ログ）の知得・利用を規律することを目的としているので、この観点は重要である。

さて、以上のような留意事項を意識しつつ、具体的な提案に移ろう。

8.2 ハード・ローに関する提言

米国に倣って、サイバーセキュリティ情報共有法の背景をなす「情報システム所有者等は、自身のシステムはもとより、文書による委託があれば他者のシステムもモニタリングできる」という原則を明記するにふさわしい法律は、次の 4 つの理由からサイバーセキュリティ基本法であろう。

① サイバーセキュリティという概念を定義づけ[158]、国家としての対応策の基本を定めた法律である。

② 第 3 条（基本理念）の第2項において、「サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促すとともに、サイバーセキュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強靱(じん)な体制を構築するための取組を積極的に推進することを旨として、行われなければならない」として、全員参加を求めている[159]。

---

[157] ソフト・ローは世界統一国家がない国際法の分野で発展したこともあり、インターネットの分野と親和性が高い（林 [2020a]）。また注 12 も参照。

[158] 第 2 条（定義）において、「サイバーセキュリティ」とは、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（「電磁的方式」）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（「電磁的記録媒体」を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること」をいうとされている。

[159] 注 154 で引用した、セキュリティを守るには、best shot（トップ・ガンによる貢献）、total effort（全員参加）、weakest point（最弱

③ 全員参加を原則としつつ、第 3 条では「重要社会基盤事業者」を「国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者をいう」と定義した上で、第 6 条（重要社会基盤事業者の責務）において、彼らに一般の法人以上の責任を期待し、システムの重要度に応じた対応を定めている[160]。

④ 他方既に 3.5 節と表 7. で明らかにしたように、「サイバー関連事業者」の概念規定は設けられているが、その範囲と責任は「重要社会基盤事業者」ほど明確ではない。

そこで自律システム管理責任を明文化するには、同法第7条を改正し、表 19. のように 2 項以下を追加すべきことを提案する（アンダーラインが改正部分）[161]。

表 19. サイバーセキュリティ基本法 7 条改正案

現行法	改正案
第 7 条 サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。	第 1 項は、現行法に同じ。 2. サイバー関連事業者は、サイバーセキュリティ確保のために、自らの管理下にある情報システム(文書による委託を受けた他者のものを含む。本条において、以下同じ)を適時モニターし、前項の努めに資するものとする。 3. 第1項のモニターにより知得した情報は、自らの管理下にある情報システムの安全性向上のために利用することができる。 4. 第 1 項のモニターにより知得した情報をもとに加工したインシデント情報は、第三者と共有することができる。 5. 前項の情報を取り扱う者は、正当な理由がなく、当該情報を漏らし、又は盗用してはならない。
第 38 条 第 17 条第 4 項又は第 31 条第 2 項の規定	第 38 条 第 7 条第 5 項、第 17 条第 4 項、第 31 条第

点の克服）のすべてが必要だとする説と合致する。

[160] 「重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする」と定めている。

[161] この提案に対して、この分野の研究者から、追加する第 2 項が「不正アクセス禁止法第 8 条のアクセス管理者による防御義務とはどのような関係になるか」「同法の規定も努力義務にとどまっており実効性が無いことをどう考えるか」というご指摘をいただいた。当面の回答として、前者に対しては「両者の目的は近似しているが、アクセス制御とモニタリングという手段が違う」と、後者に対しては「サイバーセセキュリティ基本法の全体が努力義務に多くを期待している」と、お答えしておきたい。

に違反した者は、1 年以下の懲役又は 50 万円以下の罰金に処する。	2 項の規定のいずれかに違反した者は、1 年以下の懲役又は 50 万円以下の罰金に処する。

上記によりシステム所有者の権限と責任の根拠が明確になるとしても、電気通信事業者には別途の根拠が必要であろう。なぜなら、電気通信事業者が従来のように hands-off に拘ることが許されず、notice-and-takedown 義務程度の責任を負わねばならないとすれば、hands-off の根拠規定である電気通信事業法 4 条の「通信の秘密」も、更には上位法である有線電気通信法と電波法も、見直す必要があるからである。そこで、具体的改正案として、表 20.～表 21.の提案をしたい。

表 20. 有線電気通信法と電波法の改正案（アンダーライン部分を追加）

有線電気通信法（昭和 28 年法律第 96 号）第 5 条に第 3 項・第 4 項を加え，電波法（昭和 25 年法律第 131 号）第 30 条に第 2 項・第 3 項を加える。 （技術基準） 有線電気通信法第 5 条 1 有線電気通信設備（政令で定めるものを除く。）は、政令で定める技術基準に適合するものでなければならない。 2 前項の技術基準は、これにより次の事項が確保されるものとして定められなければならない。 一 有線電気通信設備は、他人の設置する有線電気通信設備に妨害を与えないようにすること。 二 有線電気通信設備は、人体に危害を及ぼし、又は物件に損傷を与えないようにすること。 3 有線電気通信設備を設置した者は、前項の基準を達成するよう有線電気通信設備を維持・管理しなければならない。 4 有線電気通信設備を設置した者は、前項の事実を確認するために必要最低限の措置を採ることができる。この場合において当該措置を約款で公告したときには、当該措置は本法第 9 条に定める「秘密の保護」及び不正アクセス禁止法第2条第四号の「不正アクセス」の適用に関して、違法性が阻却される。 （安全施設） 電波法 30 条 1 無線設備には、人体に危害を及ぼし、又は物件に損傷を与えることがないように、総務省令で定める施設をしなければならない。 2 無線設備を設置した者は、前項の基準を達成するよう無線設備を維持・管理しなければならない。 3 無線設備を設置した者は、前項の事実を確認するために必要最低限の措置を採ることがで

きる。この場合において当該措置を約款で公告した場合には、当該措置は本法第 59 条に定める「秘密の保護」及び不正アクセス禁止法第2条第四号の「不正アクセス」の適用に関して、違法性が阻却される。

表 21. 電気通信事業法 4 条と 6 条の改正案

現行法	改正案
(秘密の保護) 第 4 条 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。 2. 電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。	第 1 項と第 2 項は、現行法に同じ。 3. 前項の規定は、事業者がサイバーセキュリティ基本法の趣旨にのっとり、サイバーセキュリティ確保のために行う必要最低限の措置を妨げるものではない。 4. 前項の措置の手続きは、省令で定める。
(利用の公平とその例外) 第 6 条 電気通信事業者は、電気通信役務の提供について、不当な差別的取扱いをしてはならない。	第 1 項は、現行法に同じ。 2 電気通信事業者は前項の規定にかかわらず、その提供する電気通信役務のために使用する電気通信設備に対して、送信型対電気通信設備サイバー攻撃を反復継続して行おうとする者に対して、電気通信役務の提供を拒否することができる。 3 電気通信事業者は第 1 項の規定にかかわらず、その提供する電気通信役務のために使用する電気通信設備を介して，刑法(明治 40 年法律第 45 号)第 168 条の 2 及び第 168 条の 3 に定める罪又はこれらの罪の未遂罪の元となる不正指令電磁的記録を送信することを、拒否することができる。 4 電気通信事業者は第 1 項の規定にかかわらず、第 2 項又は第 3 項の行為により罰金以上の刑に処せられ、その執行を終わり、又はその執行を受けることがなくなった日から 2 年を経過しない者に対して、電気通信役務の提供を拒否することができる。 5 前項の規定は、行為者が代表権を有する法人に対しても適用する。 6 電気通信事業者は、第 2 項から第 4 項の事実を確

	認するために必要最低限の措置を採ることができる。この場合において当該措置に関して本法第 44 条の定めに基づいて総務大臣に届け出る管理規定に記載し、同一の内容を約款で公告したときには、本法第 4 条に定める「秘密の保護」及び不正アクセス禁止法第2条第四号の「不正アクセス」の適用に関して、当該措置は正当業務行為として違法性が阻却される*。 7 前項の規定は、利用者の委任を受けて電気通信事業者が実施する場合に準用する。

*1.4 節で紹介した NOTICE においては、法律によって「特定アクセス」という概念を設定し、「不正アクセス」としての適用を除外しているが、本件では「違法性が阻却される」というにとどめている。

新設を提案した第 4 条 3 項以下も第 6 条 2 項以下も、サイバーセキュリティ対策という利益が、「通信の秘密」保護という他の利益に優先したり、見かけ上「利用の公平」に反する場合があることを為念的に記述したもので [162]、既存の権利を制限する意図に出たものではない。その点を明確にするため、個人データの保護を含めて、米国のサイバーセキュリティ情報共有法における「個人データの除去」のような仕組みを政令（または省令）で工夫することが望まれる。第 4 条 4 項の提案は、それを担保するための手続きを省令で定めることを義務付けるものである。

また、人権侵害を回避する視点からは、仏国が「通信の表示・分類・ルーティングのため、または迷惑メールやマルウェアの検出のために、自動処理により分析することの妨げにならない」との規定を置いたことに倣い、第 4 条3項も同様の規定とすることを検討した。しかし、変化の激しいサイバーの世界で具体的な要件を改正手続きが厳格な法律で定めると、その後の事情変更に対応できない恐れもあるので、手続き規定は省令に委ねる案とした。

ただし上記の提案は、既述の通り訴求点を絞り込んだ上でのものなので、より根源的な問題である「IoT 機器のセキュリティ対策」という視点は、敢えて回避している。総務省も経済産業省も、既に IoT 機器に対するセキュリティ問題への取り組みを行っているところであるが、その視点から表 20. や表 21. を超える提言が出ることを、むしろ期待している [163] [164]。

[162] 「利用の公平」を制限する典型的な例は、深刻なサイバー・インシデント発生時に優先順位をつけて発信を停止したり、解除したりする行為（公衆衛生における強制入院や、トリアージュに類似した行為）である。
[163] 総務省関連の事業用電気通信設備規則は、伝統的な電気通信設備に関しては良くできているが、IT デバイスや IoT 機器にそのまま適用できるか（ピッタリかどうか）には疑問がある。
[164] また IoT という新しい応用分野では、電気通信設備か否かのメルクマールよりも、ネットワーク全体や他の接続機器に悪影響を及ぼすものを回避するにはどうすべきか、という視点での省庁横断的な検討が期待される。

8.3 手続き的保障（ハード・ローとソフト・ローの橋渡し）

さて、提案の良否を判断するには省令の具体案を示さなければならないが、これを細部まで煮詰めるには共著者の知識と経験が不足している。そこで、ここでは表 22. において「骨子」のみを記述し、具体的条文などは、所管の担当者にお願いすることにしたい。

なお、本件は「通信の秘密」規定の保護下にある情報に関して、例外的に利活用できる範囲を定めるものとして、その範囲や手続きの面で慎重を期すために策定するものである。その意味では、他の業種にはない特殊事情ともいえ、総務省令で定めるのがふさわしい。しかし、サイバーセキュリティ対策が分野横断的な性格を有することに鑑みれば、将来的にはサイバーセキュリティ基本法に定めるサイバーセキュリティ協議会の参加者はもとより、サイバー関連事業者にも適用される「サイバー攻撃対策と通信の秘密」に関する準則（ソフト・ロー）として、広く参考にされることを期待したい。

表 22. 電気通信事業法 4 条の改正に伴う「必要最低限の措置」に関する手続きを定める省令案（骨子）

要素	目的	手続き的担保の骨子案	備考
1)「必要最低限」の範囲の限定	人権侵害を避けつつサイバーセキュリティ対策の実効性を挙げるため、対策の範囲を限定する。	「必要最低限の措置」は、サイバーセキュリティ基本法（以下「法」）2 条の基本理念に沿ったものでなければならない。	
2)通信ログ情報の知得	情報ネットワークの処理履歴（通信ログ）情報を知得することがサイバーセキュリティ対策の出発点であることを明記する。	電気通信事業者は、通信ログを取得し、サイバーセキュリティ事故の原因究明に役立てることができる。	情報処理事業者にとっては、表 3. の 9 原則だけで十分か？
3)通信ログ情報の守秘義務	関係者以外への情報の窃用や漏示を禁止する。	違反行為に対しては行為者が電気通信事業従事者か否かにより、「通信の秘密」侵害罪（事業法 179 条 1 項又は 2 項）が適用される。	「為念的なもので新たな規定は要しない」と考えたが、罪刑法定主義の観点から、同法 164 条 6 項を追加して規定することが望ましいか？*
4)「通信	「自律システムの所有者	上記 2) と 3) による正当な	

の秘密」との関係	(運営者を含む)によるログの利活用に関する9原則」を順守した利活用は、「通信の秘密」侵害の違法性が阻却される「正当業務行為」であることを明確にする。	行為は、正当業務行為として「通信の秘密」侵害に問われることはない。	
5)インシデント情報からの個人識別符号等の除去	プライバシー侵害のリスクを最小化するため、インシデント情報の共有には匿名加工を義務付ける。	インシデント情報を共有するには、個人情報保護法における「匿名加工情報」(同法2条9項)の要件を満たすよう加工しなければならない。	インシデント情報は、EU 指令における「リスク」の定義を基礎に「NISに悪影響を及ぼす可能性があると合理的に特定可能な状況又は事象に関する重大な情報」としたい。
6)インシデント情報の共有	関係者の間での情報共有を可能にすると同時に、その範囲を限定する。	共有できる範囲は、原情報の所有者が決めることができる。	総務省への報告義務は、現行法にあるので、そのまま。
7)インシデント情報の守秘義務	関係者以外への情報の窃用や漏示を禁止する。	インシデント情報を扱う者には、同一基準の守秘義務を課すことが望ましい。	サイバー関連事業者には、基本法 38 条(1 年以下の懲役または 50 万円以下の罰金)が適用される*。
8)自律システム管理責任者の役割	電気通信設備統括管理者は既に常置されている。	電気通信設備統括管理者の役割(法44条の4)に自律システム管理責任が含まれることを為念的に記述する。	

*この点に関しては、第9章を参照。

8.4 電気通信事業法の技術的要件等の改正

7.3 節の「要改善点」は、ネットワーク所有者等に自己あるいは他者から委託された設備を、モニタリングすることを起点にしているので、電気通信事業法 41 条（事業用電気通信設備の維持に関する規定）を再度（4.1 節に加えて）点検してみた。当初の私たちの予想では、同規定はハード的な機能不全はほぼカバーできるが、ウィルスなどによるソフト的なものは抜け落ちる可能性があるため、「その他の機能不全」を含めることとすれば、サイバー攻撃やマルウェアの影響を受けて、ネットワークが本来の機能を発揮しない場合をすべて網羅することができるのではないかと考えた。

実際の規定を精査してみた結果、法律の運用者はその点にも配慮しており、私たちの懸念はさほど重大ではないようにも思われた。しかし、なお慎重を期すのであれば、表 23. におけるように若干の文言を追加するのがベターではないかと思われる。

表 23. 現行の電気通信事業法 41 条を前提にした改正案（アンダーライン部分を追加）

（電気通信設備の維持）
第 41 条 電気通信回線設備を設置する電気通信事業者は、その電気通信事業の用に供する電気通信設備（カッコ内省略）を総務省令で定める技術基準に適合するように維持しなければならない。
2 基礎的電気通信役務を提供する電気通信事業者は、その基礎的電気通信役務を提供する電気通信事業の用に供する電気通信設備（カッコ内省略）を総務省令で定める技術基準に適合するように維持しなければならない。
3 （略）
4 （略）
5 第 1 項、第 2 項及び前項の技術基準は、これにより次の事項が確保されるものとして定められなければならない。
一 電気通信設備の損壊又は故障<u>並びにサイバーセキュリティに関するその他の機能不全</u>により、電気通信役務の提供に著しい支障を及ぼさないようにすること。
二 電気通信役務の品質が適正であるようにすること。
三 通信の秘密が侵されないようにすること。
四 利用者又は他の電気通信事業者の接続する電気通信設備を損傷し、又はその機能に障害を与えないようにすること。
五 他の電気通信事業者の接続する電気通信設備との責任の分界が明確であるようにすること。

ただし、上記の案は共著者の独創ではなく、既に存在する規律をハード・ローである事業法に格上げしたものに過ぎないともいえる。なぜなら、41 条関連については、「事業用電気通信

設備規則」6 条に[165]、また 44 条関連では、「電気通信事業法施行規則」29 条に[166]、それぞれ適切な規定が置かれているからである。

しかし 7.1 節で述べたように、電気通信の世界は技術を法が微妙に絡み合っているにもかかわらず、それぞれの専門家は異なることが多いので、この両規定を知っている従業者はさほど多くない。サイバーセキュリティが最近に至って急速に重要度を増してきた点に鑑みれば、施行規則や（より下位の）規則ではなく、「法」に規定する意味は決して小さくないと思われる[167]。

8.5 具体的提言：ソフト・ロー

前節までで、サイバーセキュリティにおける情報システム所有者等の権限と責任を明確にすることを起点に、対策の実効性を高めるための制定法の改正に関する提言は網羅したつもりである。しかし、こうした措置が実効性を有するためには原則論や精神論だけでは不十分で、ソフト・ローにおいて具体的な手順が規定され、それに従えば誰もが法を順守できるようにした置くことが望ましい。

その際、中心となるべきソフト・ローは、しばしばインターネットの安定的運用に関する協議会 [2018] として引用した「電気通信事業におけるサイバー攻撃への対処と通信の秘密に関するガイドライン（第 5 版）」となるであろう。サイバーセキュリティ対策として取り得る施策が、各種の規定にばらばらに記されていたいのでは法令順守の妨げになるので、法改正を踏まえて新たな仕組みとなる枠組みを、すべて同ガイドラインに記載することが期待される。

その場合、1.3 節で述べた「ログの利活用に関する 9 原則」を忘れず記載して欲しいので、以下に表 3. を再掲する。この原則自体は、読者の理解が得られるかと思うが、例えばバルクデータを機械処理して、どのようなプロセスを経て特定データに加工し、それを利活用できるかについては、なお曖昧さを残す点については、残念ながら認めざるを得ない。それには政治的な背景と技術的な背景の、両面がある。

前者は、情報共有の第 6 段階を想定しなければ何が正解かが分からないこと、後者は、どの段階で情報を捨てるかに関して英米の両国でもある種の差があるなどの事情である。総じていえば、英国式はインテリジェンスの役割を前面に出し（その代わり説明責任を他国よりは明確にし）、米国式はインテリジェンスとミリタリーが一体となっており（その分非公開情報が多くなり）、ブラック・ボックスも多くなると言えそうで、この論文でどちらに拠るべきか決められなかった。

---

[165] 同規則 6 条は、「電気通信事業者は、その電気通信事業の用に供する電気通信設備について、サイバー対策を含む防護措置を取らなければならない。」としており、当該防護措置の具体的内容の妥当性を「自己確認」する届出制度まで完備している。

[166] 「電気通信事業者は、その電気通信事業の用に供する電気通信設備の情報セキュリティの確保のための方針と情報セキュリティ対策の内容について、管理規程に記載しなければならない。」としている。

[167] 本来なら情報システムに関しても（為念的にせよ）同様の規定を置くことが望まれるが、情報処理振興事業法の改正を終えたばかりであり、またその基本的立場は「自律」であるため、ソフト・ローに委ねられるだろうから、所管官庁（経済産業省）における省令の行方を見守りたい。

表 3.（再掲）自律システムの所有者（運営者を含む）によるログの利活用に関する 9 原則

① 目的：サイバーセキュリティ対策に生かす場合に限る、
② バルク知得と速やかな特定データへの変換：バルクデータとして一旦知得することはできるが、精査を要する情報だけを特定した上で他は速やかに消去しなければならない、
③ 自己利用の自由：特定データは自己利用することができる、
④ 報告の奨励：精査を要するデータを匿名化してインシデント情報に加工し、所管官庁等へ報告することが奨励され、
⑤ 共有の許容：インシデント情報を他者と共有することができるが、
⑥ 匿名性の維持：捜査差押令状などの正規の要請がない限り個人識別データと突合せず、
⑦ 消去：一定期間が経過すれば復元困難な形で消去しなければならず、
⑧ 情報保全：全プロセスを通じて情報の保全に責任を負い、
⑨ 監査：全プロセスが正しく実行されているか第三者による定期的なチェックを受ける。

8.6 国際法との整合性

前節までで具体的な提言は終わり[168]、本節では、その国際法との整合性について検証する。電気通信事業は国際的な広がりを持つので、国連の機関の中で最古の歴史を誇る ITU（International Telecommunication Union=国際電気通信連合）の憲章（Constitution）、条約（Convention）、業務規則（Administration。その中でも ITR=International Telecommunication Regulations が最も関係が深い）の 3 者に関連の規定が置かれている。

これらは元来、国際電気通信にのみ適用される規定であるが、国際と国内はつながっているし、管理方法が別であると種々の問題も派生するので、一体として管理することが望ましい。また、わが国は国際機関の決定を尊重する気風があるので、電気通信に従事する者の間では、ITU の決定は国内法の基準になるとして順守されてきた。ところが、基幹ネットワークがインターネットになった今日では、インターネット・コミュニティ（代表は、ISOC=Internet SOCiety[169]）の各種規律とも無縁ではいられない。

両者の理念は大筋では合致しているものの、既に 1.4 節で述べたメンタリティの差もあってか、時に対立することもある。両者が最も先鋭に対立したのは、電気通信に関する国際的な規律のあり方を担う ITU が、ITR の改正を検討した 2102 年の WCIT（World Conference for International Telecommunication）においてであった。

この会議では、セキュリティを含む国家の規制をどこまで認めるべきかが焦点になり、次の諸点が対立の火種になったとされる（総務省パワーポイント [2013][170]）。

---

[168] なお前章で「要改善点」と指摘した事項のうち、以下のものについては、それぞれの事情で時差をおいた対応が望ましいと考えたため、本稿では具体案を示していないことを、ご了解いただきたい。a）インシデント情報の所管官庁への報告、b）インシデント情報共有の手続き、c）共有促進策。

[169] 1992 年に設立された国際的な非営利組織で、“The Internet is for everyone.” というビジョンに基づいて活動している。

[170] 上記のほか、a）政府によるインターネット上の表現（コンテンツ）に対する検閲・遮断等に関する規定を追加すべきか、b）イン

① ITR の目的及び範囲に「セキュリティ」を追加すべきか。
② 現行 ITR の規律の対象である国際通信回線設備を設置する電気通信事業者に加え、インターネット・サービス提供事業者にまで、対象を広げるべきか。
③ 国による情報規制を含むセキュリティの確保に関し、電気通信事業者に義務を負わせることとすべきか。
④ 無差別かつ大量に一括送信されるスパム（迷惑メール）に関し、国や電気通信事業者にスパム拡散防止を義務付けることとすべきか。

これらの諸点は相互に関連しており、「インターネットには自律的管理によって十分機能しているから、電気通信の国際規約等で規律する必要はない」とする米国と、「インターネットが基幹ネットワークとなった現代では、国家主権との関係を調整するのは当然で、ITR に必要な条文を入れるべきである」とするロシア・中国等が決定的に対立した[171]。

この間にあって EU やわが国は、「A. 表現の検閲につながるような規制を採るべきではない」が、「B. コンテンツに関わらない物理的なネットワークのセキュリティに関しては、国家の過度な介入は避けるべきである一方、事業者の対応強化が望まれるため、事業者に適切な措置を（義務付けではなく）奨励する旨の規定を追加すべきである」との調整案を提示したが、原則論に拘る両陣営の妥協を引き出すことができなかった模様である（総務省パワーポイント[2013]）。

結局、ITR はロシア・中国や開発途上国の多数で可決されたが、西欧先進諸国は反対のため署名せず、署名した国は 89 か国、署名しなかった国は 55 か国という、ITU 史上初めてと思われる「split decision かつ西欧先進諸国が少数派」という結果になった。ITR 自体は 2015 年 1 月 1 日から施行されたが、署名しなかった国が改めて不同意（不参加）の通知を行った場合、改正 ITR はこれらの国に適用されず、現行の ITR が適用されるという変則事態になっている。

それもあってか、会議終了直後の 2012 年 12 月 15 日における総務省の報道発表は、以下のように素気ないものであった。

https://www.soumu.go.jp/menu_news/s-news/01tsushin06_02000042.html

> 平成 24 年（2012 年）12 月 3 日（月）から 14 日（金）までの間、電気通信に関する国際連合の専門機関である国際電気通信連合（ITU）において、各国政府を法的に拘束する国際電気通信規則（ITR）を改正する世界国際電気通信会議（WCIT）が、アラブ首長国連邦（ドバイ）で開催され、ITR の改正文書が採択されました。我が国は、署名を見送ることとしました。

このように国連機関の模範とされた ITU が分断の危機に瀕していることは憂慮すべきことで

ターネット・サービス提供事業者にインフラ投資の費用を負担させるため、流通情報量に見合う料金を課すべきか、c) 携帯電話の国際ローミング料金に関して、国や電気通信事業者に、料金の通知（透明性）や低廉化の義務を課すべきか等も、論議を呼んだとされる。

[171] なおロシアは、インターネットのガバナンスに関しても追加提案を行った。

ある。しかし本稿の目的に絞った見方からすれば、本稿で主張している「コンテンツ（間接）責任」と「自律システム管理責任」の一環としてのサイバーセキュリティ対策をアンバンドルすることと、後者に関して電気通事業者とその他の自律システム所有者等の権限と責任を（強制にならない程度に）明確化するという提言は、上述のわが国の調整案における A.と B.とを共に満たすものとなっているので、少なくとも西欧先進諸国とは同一歩調が取れるとの自信を与えてくれる。

9　提案の自己点検—刑事罰の横断的比較

9.1 刑事罰の横断的比較表

本稿の最後に、私たちの改正提案を現行法の体系の中に位置づけて、相互に矛盾はないか、新たな問題を生み出していないかを検証しておきたい。「通信の秘密」をアンバンドル（分節化）することは部分最適を目指すことを意味するので、部分間の不整合を拡大させ、全体最適を妨げかねないからである。

具体的点検項目としては、謙抑性が最も強く要請される刑事罰を取り上げることとしたい。現行法と改正提案が、ログの知得から自己利用、インシデント情報としての報告を含めた共有、最終的には廃棄というライフ・サイクルの全過程を通じて、窃用等の違法行為に対する罪をどのように規定しているかを比較すると、表 24. が得られる [172]。以下、この表を中心に検討を進めよう。

表 24.「通信の秘密」関連情報に関する窃用等の罪

根拠法 ＼ 項目	有線法	電波法	事業法（狭義の電気通信事業）	同（適用除外電気通信事業）	同（みなし規定）	サイバーセキュリティ基本法
適用対象	有線電気通信	無線通信	電気通信事業	適用除外電気通信事業（164 条 1 項）	認定送信型対電気通信設備サイバー攻撃対処協会の業務（116 条の 2 以下）	サイバー関連事業者（7 条）

[172] 「通信の秘密を侵す」には、「情報の不正な知得・窃用・漏示」の 3 つの態様が含まれるとの説が通説であるが、無線通信では「知得」自体は罪にならないなどのバリエーションがあるので、すべてに共通の「窃用」を代表例とした。

保護対象情報	有線電気通信の秘密(9条)	無線局の取扱中に係り、特定の相手方に対して行われる無線通信の秘密(59条、109条)*	電気通信事業者の取扱中にかかる通信の秘密(事業従事者の場合は「在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密」も含む)(4条1項、2項)	同左(164条3項)	協会が行う第116条の2第2項第一号ロの通知(164条4項)及び第116条の2第2項第二号ロの通信履歴の電磁的記録(164条5項)並びに送信型対電気通信設備サイバー攻撃対処業務に関して知り得た秘密(116条の4)	モニターにより知得した情報及びそれを加工したインシデント情報(提案した7条3項・4項)
違反行為	知得、窃用、漏示のいずれも(14条)	窃用と「存在又は内容の」漏示(59条)	知得、窃用、漏示のいずれも(4条の解釈)	知得、窃用、漏示のいずれも(4条の解釈)	知得、窃用、漏示のいずれも(4条の解釈)	正当な理由がなく、秘密を漏らし、又は盗用する行為(17条4項)
行為者	何人も	何人も	何人も	何人も	何人も	サイバー関連事業において「モニターにより知得した情報」を取り扱う者(提案した7条5項)
刑罰(一般人の場合)	2年以下の懲役又は50万円以下の	1年以下の懲役又は50万円以下の	2年以下の懲役又は100万円以下の罰金(179条1項)	同左(179条1項)	同左(179条1項)	該当せず

	罰金(14条1項)	罰金(109条1項)				
刑罰(事業従事者の場合)	3年以下の懲役又は100万円以下の罰金(14条2項)	2年以下の懲役又は100万円以下の罰金(109条2項)	3年以下の懲役又は200万円以下の罰金(179条2項)	同左(179条2項)	同左(179条2項)	1年以下の懲役又は50万円以下の罰金(38条)
法人に関する両罰規定	なし	なし	あり(190条)	同左(190条)	同左(190条)	なし

*他に暗号通信の復元も禁じられる(109条の2)。

9.2 事業法、有線法、電波法間の異同

「通信の秘密」保護と刑事罰の規定は、事業法におけるもののほか、有線法と電波法にも同種の規定があるので、これら3法の規定を比較してみよう。3つの法律における共通点は、「通信の秘密」の保護の規定と[173]、「通信の秘密」の侵害行為に対する刑罰規定とが対となっていることが挙げられる。また事業・業務の従事者と従事していない者とでは、「通信の秘密」の侵害行為を行った場合の刑罰の重さに差が設けられていること(事業従事者に対する加重)も、共通している。

他方で、3者は以下の5点において相違がある。

① 保護対象は、事業法では「電気通信事業者の取扱中に係る通信」、電波法では「無線局の取扱中に係る無線通信」であるが、有線法では「有線電気通信の秘密」であり、文言上は「取扱中」の限定がない。また「通信の秘密」の侵害行為類型としては、知得、窃用、漏示の3つがあるとされているが、無線法では電波の特性上、何人でも偶然傍受することがあり得るので、知得自体に可罰性はないとされている。暗号通信の場合に、その内容復元が処罰対象になっている(109条の2)のは、単なる知得を超える行為と捉えているものと思われる。

[173] 有線法では有線電気通信の秘密、電波法では無線通信の秘密との用語となっているが、これはそれぞれの法の適用範囲を明確にするためである。

② 事業・業務の従事者の順守義務について、事業法では「電気通信事業者の取扱中に係る通信に関して知り得た他人の通信を守らなければならない（事業法 4 条 2 項）」、無線法では「無線通信の業務に従事する者が、その業務に関し知り得た前項の秘密を洩らし、又は窃用」（無線法 109 条 2 項）と規定されていて、「業務上知り得た秘密」の順守が求められているのに対して、有線法では「有線電気通信の業務に従事する者が前項の行為（注：有線電気通信の秘密を侵した）をしたときは（有線法 14 条 2 項）」となっていて、通信の秘密と（業務上）知り得た秘密の区分は設けられていない。

③ 従事者に「知り得た秘密」の順守を求めていることは、事業法と電波法では共通しているが、事業法では「通信の秘密」と「他人の秘密」の用語が用いられているのに対して、電波法ではこの用語を用いずに「業務に関し知り得た秘密」との用語が用いられている。この点に関しては、9.4 節で改めて論ずる。

④ 従事者の順守義務の期間について、事業法では在職中に加えて「その職を退いた後」も対象としている。これに対して、有線法および無線法では「通信の秘密」の侵害行為を禁止するに留まっていて、在職中とか退職後との期間に関する言及はされていない[174]。

⑤ 刑罰量刑の重さは事業法と有線法は同じであるが、電波法では事業法・有線法よりも量刑が軽くなっている。

以上の比較を通して明らかになったことは、主に以下の 2 点かと思われる。第 1 は、事業法、有線法、電波法の 3 つ法律はいずれもすべての人が順守すべき規定として、「通信の秘密」の規定を置き、事業従事者の侵害行為に対して非従事者よりも刑罰を重くしていることは共通しているが、総じて事業法がより厳格な順守義務を課しているように思われる。これは電気通信全体の中で、「業として」これを行うことが一般化していることから、妥当と考えられる。

第 2 点は、「通信の秘密」と「業務上知り得た秘密」が保護対象の 2 大類型であるが、後者については他の業法や、各種の行政法規などに同種の規定が見られるので、その間の均衡を検証する余地があることである。現時点で即断することは危険であるが、機会を捉えて試みてみたい。というのも、情報法（特に、その総論部分）は未発達であり、「情報に関する権利・利益の侵害に対して、どのように対処すべきか」は、この分野の理論の発展にとって不可欠の視点だからである（林 [2017a]）。

9.3 事業法における 3 類型と刑事罰

1.2 節で述べたように、事業法 4 条は電気通信事業を名宛人にしたものであるが、同法 164 条 1 項の電気通信事業（適用除外電気通信事業）は事業法の他の規定の適用は除外されるものの、3 条（検閲の禁止）と 4 条の規定は適用されることになっていて、当該事業に係る「通

[174] もっとも刑事罰に限っていえば、「長期 5 年未満の懲役若しくは禁錮又は罰金に当たる罪」の公訴時効は 3 年であるので（刑事訴訟法 250 条 2 項六号）、3 法間の実質的な差は僅少であると思われる。

信の秘密」の侵害行為に対しては、同法 179 条の刑罰が適用される。

加えて 2018 年改正事業法において、サイバー攻撃への対応力強化のために、「認定送信型対電気通信設備サイバー攻撃対処協会（2 章 8 節 116 条の 2～116 条の 8）」（以下、協会）の規定が新設され、協会の特定業務およびその業務の従事者に関しては、それぞれ「電気通信事業者の取扱中に係る通信」および「電気通信事業に従事する者」とみなすという規定が新設された（同法 164 条 4 項・5 項。林・田川 [2018]）この規定に基づいて協会の電気通信事業者の取扱中の通信とみなされた特定業務に対する侵害行為に対しては、179 条の刑罰が科される。

従って、事業法の「通信の秘密」に関する「刑」の面から見ると、事業法 4 条、164 条 1 項、164 条 4 項・5 項の 3 類型があることになるが、これを「罰」の面から見ると、いずれも 4 条の遵守義務および 179 条の罰則が適用されるので、事業法内での違いはない。

9.4 事業法における「通信の秘密」と「他人の秘密」の区分

9.2 節の ③ で指摘した、4 条 1 項の「通信の秘密」と「他人の秘密」の区分については、2 つの解釈が考えられる。1 つは「通信の秘密」よりも「他人の秘密」の範囲が広いという見方である。しかし「通信の秘密」ではないが「他人の秘密」には該当する例として過去に挙げられたのは、人相（電報を窓口で受け付けた場合）、言葉の訛り（通話を交換手が媒介した場合）、プッシュホンに記憶された相手番号等、かなり限定的である。加えて、これらは電話利用の例であって、インターネット利用の例は挙げられておらず、現在では両者の差分がほとんどないと考えられる。

そこで他の解釈は、1 項と 2 項では規律対象者と順守義務が異なると理解するものである。すなわち 1 項は電気通信事業の従事者以外の者に対する規定であり、知得・窃用・漏えいのすべてが禁止されているのに対して、電気通信事業の従事者は「通信の秘密」に該当する情報を業務遂行のため知得するが、これは正当業務行為であって違法性が阻却される。そこで 2 項では、電気通信事業の従事者は「通信の秘密」に該当する情報を知得することができるが、その知得した「他人の秘密」を守らなければならないと規定されているとするものである（この区分の詳細については、林・田川 [2018] 参照）。

つまり事業法 4 条 1 項と 2 項では、秘密の保護対象はいずれも「電気通信事業者の取扱中に係る通信」に関するものであり、2 項において従事者は「取扱中に係る通信に関して知り得た他人の秘密」の順守が求められる。

従事者が業務遂行上知り得る秘密は、上記の「他人の秘密」以外にも、契約者情報（1.2 節における C）などがあるが、これらの情報を自己の利益のために窃用したり、部外に漏えいしても、「取扱中の通信」に係る秘密を窃用したり、漏えいしたりしているわけではないので、4 条 2 項違反とはならない。

また「通信の秘密」には当たらないが「他人の秘密」に該当する情報を窃用、漏示した場合は、4 条 2 項違反にはなるが、それに対する責任は民事上（損害賠償等）・服務上のもの（懲戒処分等）に止まり、事業法 179 条の刑事罰は科せられないと解釈されている[175]。

9.5 事業法と基本法の比較

一方、基本法 7 条の改正提案において、サイバー関連事業者は自らの管理下にある情報システムをモニターし（2 項）、それにより知得した情報を自らの管理下にある情報システムの安全性向上のために利用でき（3 項）、この情報を加工したインシデント情報を第三者と共有できること（4 項）を提案している。またインシデント情報を取り扱う者は守秘義務を負い（5 項）、違反には刑事罰（38 条改正による 1 年以下の懲役又は 50 万円以下の罰金）を科すとの改正提案を行っている。

この量刑は、「通信の秘密」の侵害に対する事業法 179 条の罰則よりも軽くなっている。また「通信の秘密」は従事者だけではなく、すべての人の義務であるのに対して、基本法の罰則は特定業務の従事者が守秘義務のある情報を漏らしたり、盗用したりした場合に適用されるもので、従事者以外が当該情報を漏えいしたり盗用したりしても 38 条の罰則の対象外となる。そこで、従事者以外の者が窃取、漏えいした場合の当該情報の保護のあり方が問題になる。

これに対しては、2 つの対処策が考えられる。第 1 は現行法で対処する方法で、一般の不法行為責任（民法 709 条）を追求する方法である。第 2 は、現行法では保護の程度が不十分であると考えて、新たな立法措置によって、民事責任、さらには刑事責任も追及するという方法である。

このどちらの方法が良いかは、共有情報の保護の必要性をどの程度であると考えるかで決まってくると考えられる。本稿ではログを知得、分析してインシデント情報に加工し、そのインシデント情報の共有を行って、サイバーセキュリティを強化することを一つの柱としている。そこで例えば、サイバー攻撃を意図している第三者がインシデント情報を取得して、その情報をサイバー攻撃に利用する可能性およびその情報を利用することがサイバー攻撃をどの程度容易にするかの判断によって、保護のレベルをどう設定したら良いかが決まってくる（この点は、次節で述べる「限定提供データ」の窃用・漏えいに刑事罰を科すべきかという論点と結びついてくる）。

またサイバー攻撃の意図・動機は、愉快犯、経済的利益追求、企業等の営業情報（機密情報）や国家機密情報の窃取、あるいは重要インフラの可用性の喪失など多様であるが、

---

[175] 罪刑法定主義に忠実に従えば、この解釈が正しいと思われる。現に電気通信法制研究会［1987］は以下のように説明していたが、その後この点に直接触れたものはない。「（電気通信事業法）第 4 条の第 1 項と第 2 項の関係については、第 2 項は電気通信事業者に従事する者について、職務上正当行為としての知得行為は違法性がないこと、守るべき範囲は、通信の構成要素以外のものであってもそれを推知させるものを含むという第 1 項に対する特則を定めたものである。他方罰則の適用関係については電気通信事業に従事する者について本条第 1 項の『通信の秘密を侵した』場合に加重罰を科することとしている（第 2 項）。したがって、通信の秘密の構成要素以外の他人の秘密を守らないことに対しては罰則の適用はなく、民事上・服務上の責任を問われるにとどまる。（以下略）」（pp.267-268）。

窃取される情報や可用性の喪失による損害の程度も区々であると考えられる。さらに、愉快犯のように自分の技術力を誇示するために情報を窃取する場合には、実際の被害（損害）は愉快犯が窃取した情報を悪用しない限り大きくはないと考えられる。

9.6 限定提供データの意義

このようにサイバー攻撃といっても、その内実はさまざまであって、攻撃者の意図（動機）によって共有情報の保護の程度も変わり得ると考えられる。この保護レベルを検討するために、2018 年の改正不正競争防止法で新設された「限定提供データ」（2 条 7 項に定義）の規定が参考になる。「限定提供データ」というのは、他者との共有を前提に一定の条件下で利用可能な情報である。例としては自動運転用地図データ、POS システムで収集した商品毎の売上データなどが示されている [176]。

限定提供データは、企業間で複数者に提供や共有されることで、新たな事業の創出につながったり、サービスや製品の付加価値を高めるなど、その利活用が期待されるデータである。このように価値あるデータであっても、著作権の対象ではなく、「営業秘密」にも該当しないので、現行法では保護されないことになるが、不正な流通が生ずると被害は急速にかつ広範囲に拡大する恐れがあるために、新たに不正競争防止法に「限定提供データ」の概念が導入された。

また契約に基づく自由な取引を前提とし、通常の正当な事業活動を阻害しない範囲で、悪質性の高い、不正取得・不正使用等への救済措置として、法的な保護が与えられるようになった。ただし、データベース著作物や営業秘密に関しては、民事措置（差止と損害賠償）と刑事措置（懲役・罰金）が認められるのに対して、「限定提供データ」では民事措置のみが認められていて、刑事措置は認められておらず、営業秘密等とは法的保護レベルが異なる [177]。

9.7 サイバーセキュリティ強化のための情報共有を促進する法制度整備

ログを知得、分析してインシデント情報に加工し、その情報を共有してサイバーセキュリティ強化に役立てる動きが従来さまざまな組織で行われてきたが、2018 年の改正基本法 17 条でサイバーセキュリティ協議会（以下、協議会）の規定が新設され、2019 年 4 月に発足した。この協議会で法律の根拠を有する形でインシデント情報の共有を行って、サイバーセキュリティの強化の動きが本格化することが期待されている。

基本法 17 条において協議会の特定業務に関して守秘義務を課す現行法の規定に加えて、表 19 の改正提案の趣旨は、サイバーセキュリティ強化のために、同法 7 条のサイバー関連事

[176] 2019 年 1 月 23 日経済産業省作成の「限定提供データ管理指針」p.12 以下
https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pd
[177] もっとも不正競争防止法で保護される行為には、制定当初は民事救済（損害賠償と差止）しか認められなかったものが、その後の改正で刑事罰を伴う保護が加えられたものがあるので、将来のあり方は十分議論していく必要があろう。

業者全体に情報共有を促進するとともに、守秘義務を課して、共有情報の安全な利活用を実現しようとするものである。

7.5 節で述べたように、協議会の会員メンバーには情報共有することで不利益を被る恐れを有する者がいて、共有に対する不安があることが伺える。情報共有を促進するためには、守秘義務によって安全な活用を図るだけではなく、情報共有によって他の法令違反に問われる恐れがないようにするために、CISA にあるように情報共有に関する免責規定などを整備することも検討課題であると考えられる。

その 1 つの方法として、前節で述べた「限定提供データ」の制度を使って、インシデント情報の共有を行うことは可能だろうか。法制定者が想定したユース・ケースは先に述べたような例であり、インシデント情報は視野に入っていないが、a) 有用性、b) 非公知性、c) アクセス制限性、の要件は満たすと思われるので [178]、十分検討に値すると思われる。この制度は不正競争防止法の所管である経済産業省が主導したもので、更にその内部でも知財部門が担当しているため、専門外の者には周知が行き届いていないが、サイバーセキュリティ研究者の早急な検討を促したい [179]。

9.8 検証結果のまとめと若干の留保

今回共著者が提案した法改正のうち「通信の秘密」侵害罪に関連する部分は、ハード・ローとしての基本法 7 条の改正と、ハード・ローであるがソフト・ローとの橋渡しの機能を併せ持つ、事業法 4 条の改正に伴う省令案（表 21. の改正 4 条提案を受けた、表 22. の省令案）の 2 つである。

基本法 7 条に関する守秘義務のうち、3 項の「（加工前の）通信ログ」に関する部分は「通信の秘密」に係る情報であると考えられ、違反行為に対する罰則は事業法 179 条に既に法定されている。一方 4 項と 5 項の「（加工後の）インシデント情報」に関する規定は、今回の提案で初めて導入された概念であり、本来なら基本法に「業務上知り得た秘密」に準ずる罰則を規定するのが、妥当ではないかと思われる。

しかし現在の案は、基本法 7 条 3 項の「（加工前の）通信ログ」に関する部分は「通信の秘密」に係るので、事業法に関する省令によって事業法の対象外であるサイバー関連事業者に関する規定を入れて罰則を課す一方、4 項と 5 項の「（加工後の）インシデント情報」に関しては、サイバー関連事業者には基本法 38 条が適用されるとするものの、サイバー関連事業者以

[178] 営業秘密の 3 要件は、a) 有用性、b) 非公知性、c) 秘密管理性、の 3 つであるところ、限定提供データには c) と同じ強度の管理性は求められていない。しかし、それに代わって ID・パスワードなどの技術的な管理を施して提供されることを求めている。

[179] 情報法の研究者の視点から見れば、限定提供データが提起する問題は、以下の 4 点から極めて注目すべきものと思われる（林 [2017a]、福岡・松村 [2019]）。a) 情報を法的に保護する仕組みとしては知的財産型と秘密保護型があるところ、両者は明確に区分されていてハイブリッド型は存在しないものとされてきた、b) 総じていえば知財型の理論は成熟しつつあるのに対して、秘密型の理論は（研究者も少なく）十分な展開を見せていない（林 [2005b]）、c) このような中で米国においては秘密型の典型である classified information の周辺に CUI（Controlled Unclassified Information）というハイブリッド型の保護方式が登場した、d) わが国の限定提供データも、CUI 類似のハイブリッド型保護の要素を持っている。

外には適用条文がない状態となっている。

事業法 4 条 1 項の「通信の秘密」の順守義務の名宛人はすべての人なので、事業法の対象外であるサイバー関連事業者に関する規定を省令に入れることは、必ずしも不適当とは言えないと思われる。しかし、インシデント情報は通信ログを分析・加工したもので、もはや「通信の秘密」に係る情報そのものとは言えないことから、事業法省令と基本法の間で守秘義務違反に関する罰則規定が整合性を欠いているのではないか、との疑念が生ずる。

この差は「情報の加工度」によって説明できるのではないかと考えるが、そのように主張すれば、基本法 7 条改正案のうち 3 項と 4 項・5 項の組合せ（「モニターにより知得した情報」と「それをもとに加工したインシデント情報」）の差、そのものの妥当性（共著者は、3 項は「通信の秘密」に該当し、4 項・5 項は該当しないと考えている）が問われることになろう。

この点以外にも、共著者の提案には未熟で検討不足の部分が多々あるかもしれない。私たちは「合格ラインの 60 点すれすれでも良いから議論を喚起したい」という気持ちで、問題提起の論稿として本論文を提出しているので、そうしたご指摘には謙虚に耳を傾けるつもりである。本稿の草稿段階でコメントをいただいた各位に感謝するとともに、読者の皆様から、数多くのご批判・ご叱正をいただけることを期待している。

参考文献

[1] 生貝直人 [2011]『情報社会と共同規制： インターネット政策の国際比較制度研究』勁草書房

[2] 石井夏生利 [2020]『EU データ保護法』勁草書房

[3] 伊藤真・前田哲夫 [2017]「サイトブロッキングと通信の秘密」『コピライト』No.690

[4] 井上正仁 [1997]『捜査手段としての通信・会話の傍受』有斐閣

[5] インターネットと通信の秘密研究会（第 1 期） [2013]『インターネット時代の「通信の秘密」再考』 http://lab.iisec.ac.jp/~hayashi/20130608Report.pdf

[6] インターネットと通信の秘密研究会（第 2 期） [2014]『インターネット時代の「通信の秘密」各国比較』 http://lab.iisec.ac.jp/~hayashi/2014-7-7.pdf

[7] インターネットの安定的運用に関する協議会 [2018]「電気通信事業におけるサイバー攻撃への対処と通信の秘密に関するガイドライン（第 5 版）」 https://www.jaipa.or.jp/topics/2018/11/post-16.php

[8] 金光昭・吉田修三 [1952]『公衆電気通信法解説』日信出版

[9] 警察政策学会 [2015]『米国国家安全保障庁の実態研究』（警察政策学会資料 82 号、茂田忠良筆）

[10] 笹川平和財団 [2018]「日本にサイバーセキュリティ庁の創設を」 https://www.spf.org/global-data/cyber_security_2018_web.pdf

[11] 情報セキュリティ大学院大学 [2014] 「インターネットと通信の秘密」研究会(第 2 期）報告書『インターネット時代の「通信の秘密」各国比較』

http://lab.iisec.ac.jp/~hayashi/2014-7-7.pdf
[12] 情報セキュリティ大学院大学[2017]「英国 IPA（Investigatory Powers Act）2016 に関する調査報告書」 http://lab.iisec.ac.jp/~hayashi/170612%20IPA2016.pdf
[13] 島村智子 [2018]「ネットワーク・情報システムの安全に関する指令（NIS 指令）」『外国の立法』277 号
[14] 総務省パワーポイント [2013]「WCIT-12 の結果について」 https://www.soumu.go.jp/main_content/000195974.pdf
[15] 曽我部真裕 [2019]「フランスの『デジタル共和国法』について」『法律時報』91 巻 6 号
[16] 高嶋幹夫（著）、藤田潔・高部豊彦（監修）[2015]『実務 電気通信事業法』NTT 出版
[17] 高橋郁夫・林紘一郎・舟橋信・吉田一雄 [2009] 「通信の秘密の数奇な運命（制定法）」『情報ネットワーク・ローレビュー』第 8 巻
[18] 多賀谷一照 [1995]『行政とマルチメディアの法理論』弘文堂
[19] 多賀谷一照・岡崎俊一・岡崎毅・豊島基暢・藤野克（編著）[2008]『電気通信事業法逐条解説』電気通信振興会
[20] 田川義博 [2013] 「インターネット利用における『通信の秘密』」『情報セキュリティ総合科学』vol. 5 http://www.iisec.ac.jp/proc/vol0005.html
[21] 田川義博,・林紘一郎 [2017]「サイバーセキュリティのための情報共有と中核機関のあり方―3 つのモデルの相互比較とわが国への教訓― 」『情報セキュリティ総合科学』Vol. 9 http://www.iisec.ac.jp/proc/vol0009.html
[22] 田村善之 [2019]『知財の理論』東京大学出版会
[23] 出口岳人 [2013]「世界電気通信会議（WCIT-12）結果報告（総括）」『ITU ジャーナル』Vol. 43, No. 3
[24] 電気通信法制研究会 [1987]『逐条解説 電気通信事業法』ぎょうせい
[25] 豊田透 [2017]「フランスにおける国の情報監視活動を規定する法律」『外国の立法』272
[26] 中野目善則 [2020]「サイバー犯罪の捜査と捜査権の及ぶ範囲－プライヴァシーの理解の在り方、法解釈の在り方、他国へのアクセス」『警察政策』Vol. 22
[27] 永野秀雄 [2016]「米国におけるサイバーセキュリティ法制の展開と現状―国家安全保障上の不可欠な制度基盤としてー」桜川ほか（編著）『国家安全保障と国際関係』内外出版
[28] 永野秀雄[2020]「米国国防総省におけるサイバーセキュリティ成熟度モデル認証（CMMC）の導入―現行の NIST SP 800-171 の遵守制度を超えてー」『CISTEC Journal』No. 186
[29] 成原慧 [2018a]「SOPA/PIPA 法案をめぐる米国の議論と我が国への示唆」 知的財産本部 海賊版対策タスクフォース ヒアリング資料, 2018 年 9 月 13 日
[30] 成原慧 [2018b]「海賊版サイトのブロッキングをめぐる法的問題」『法学教室』No. 453
[31] 林紘一郎 [1984]『インフォミュニケーションの時代』中央公論社
[32] 林紘一郎 [1989]『ネットワーキングの経済学』NTT 出版
[33] 林紘一郎 [1998a]『ネットワーキング：情報社会の経済学』NTT 出版

[34] 林紘一郎 [1998b]「システム思考と『ヨコ社会』の強み」『経済セミナー』No. 523 小特集「アメリカはニュー・エコノミーか」
[35] 林紘一郎 [2002]「インターネットと非規制政策」林紘一郎・池田信夫（編著）『ブロードバンド時代の制度設計』東洋経済新報社
[36] 林紘一郎 [2005a]『情報メディア法』東京大学出版会
[37] 林紘一郎 [2005b]「「秘密」の法的保護と管理義務：情報セキュリティ法を考える第一歩として」『富士通総研研究レポート』富士通総研経済研究所 No.243
https://www.fujitsu.com/jp/group/fri/report/research/2005/report-243.html
[38] 林紘一郎 [2015]「サイバー攻撃と防御における非対称と解決の可能性」『第 48 回安全工学研究発表会予稿集』安全工学会
[39] 林紘一郎 [2017a]『情報法のリーガル・マインド』勁草書房
[40] 林紘一郎 [2017b]「サイバーセキュリティ事故情報共有のあり方」『情報通信学会誌』34 巻 3 号
[41] 林紘一郎 [2020a]「サイバーセキュリティと国際法・国際政治」『ITU ジャーナル』Vol. 50, No. 1
[42] 林紘一郎 [2020b]「情報法の観点から：検閲の禁止・通信の秘密・利用の公平など」『L&T』2020 年 3 月号
[43] 林紘一郎・鈴木正朝 [2008]「情報漏洩リスクと責任」『法社会学』69 号
[44] 林紘一郎・田川義博 [1994]『ユニバーサル・サービス』中央公論社
[45] 林紘一郎・田川義博 [2016]『サイバーセキュリティにおけるバルクデータの意義』『情報セキュリティ総合科学』vol. 8
http://www.iisec.ac.jp/proc/vol0008/hayashi-tagawa16.pdf
[46] 林紘一郎・田川義博 [2018]「サイバー攻撃の被害者である民間企業の対抗手段は どこまで可能か：日米比較を軸に」『情報セキュリティ総合科学』vol. 10
http://www.iisec.ac.jp/proc/vol0010/hayashi-tagawa18.pdf
[47] 林紘一郎・田川義博 [2019] 「サイバー攻撃対策としてのログの知得・利用と『通信の秘密』」『情報セキュリティ総合科学』vol. 11 http://www.iisec.ac.jp/proc/index.html
[48] 平野晋 [2014]「免責否認の法理（『通信品位法』230 条）：イースターブルック（主席）裁判官担当 GTE Corp.「Craigslist」事件から、コジンスキー主席裁判官担当の Roommates.com 事件まで」『情報通信政策レビュー』第 8 号
[49] 福岡真之介・松村英寿 [2019]『データの法律と契約』商事法務
[50] 堀部政男 [2019a]「日 EU 間の個人データの円滑な移転実現への道程と今後の課題（上）」NBL No.1148
[51] 堀部政男 [2019b]「同（下）」NBL No.1149
[52] プール，イシエル・デ・ソラ，堀部 政男 (訳) [1988]『自由のためのテクノロジー：ニューメディアと表現の自由』東京大学出版会
[53] 松尾陽（編）[2017]『アーキテクチャと法』弘文堂
[54] 山口厚 [2015]『刑法（第 3 版）』有斐閣

[55] 吉国一郎ほか（編）[2009]『法令用語辞典（第9次改訂版）』学陽書房

[56] レッシグ、ローレンス、山形浩生・柏木亮二（訳）[2001]『CODE：インターネットの合法・違法・プライバシー』翔泳社

[57] Cannon, Robert [2012] 'The Intersection of the Electronic Communications Privacy Act and the Open Internet's 'Reasonable Network Management' Exception," submitted to TPRC（Telecom Policy Research Conference）SSRN-id2032252.pdf

[58] Harper, Jim [2005] 'Against ISP Liability' "Regulation" Spring

[59] Kerr, Orin [2015] "How does the Cybersecurity Act of 2015 change the Internet surveillance law" https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/

[60] L&T 座談会 [2020]「プラットフォーマーの法律問題―政府におけるプラットフォーム事業者規制の検討を踏まえて―」『Law & Technology』87 号

[61] Lichtman, Douglas Gary, and Eric Posner [2004] 'Holding Internet Service Providers Accountable' (John M. Olin Program in Law and Economics Working Paper No. 217)

[62] Ohm, Paul [2010] 'When Network Neutrality Met Privacy,' "Communications of ACM," Vol.53, No. 4 https://cacm.acm.org/magazines/2010/4/81488-when-network-neutrality-met-privacy/fulltext

[63] Saltzer, Jerome H., David P. Reed, & Dana Clark [1984] 'End-to-End Arguments in System Design,' Communications of the ACM

[64] Varian, Hal [2004] 'System Reliability and Free Riding,' in L. Jean Camp & Stephen Lewis (eds.) "Economics of Information Security," Kluwer Academic Publishing