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」

林　紘一郎*，田川　義博†

概 要

「通信の秘密」は，プライバシーや言論の自由を守るとともに，通信システムそのものへの信頼を担保する重要な概念である．しかし，その保障は絶対的なものではなく，他に優越する法益や，「通信の秘密」そのものと相補的な利益があれば，制限あるいは補正される場合がある．現にわが国においても，各種の例外規定が設けられ，実際に運用されている．

しかし，これらの措置は「通信の秘密」保持という原則に対して，その例外という位置づけになる．戦前の苦い検閲の歴史を持つわが国では，実務上「通信の秘密」は「検閲の禁止」と同様，高度の不可侵性を持つとされてきたので，例外措置もアド・ホックなものと理解され，それらを統一的に把握し分節化（アンバンドル）した議論はまれであった．

本稿は，このような「議論の空白」を埋めるため，以下の 6 点にわたるアンバンドルを試みる．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（通信履歴)」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，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「ユーザの同意」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「バルクデータ」の扱いを別にする．

その上で本稿の焦点は，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を念頭に，ログの知得・利用を違法・有害情報に対する「違法性阻却」とは「別建て」とする案を検討する。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）を探る．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適正運用をどのように担保するかである．

* 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

なお残念ながら ⑥ においては，さし向き特定データを念頭に置き，バルクデータは今後の課題とせざるを得なかった. これはわが国のインシデント情報の共有が，現状では官民一体型の段階にあり，政府対応力を強化した官民一体型を将来の課題としていることに対応している.

1 問題の所在

1.1 インターネットの光と影

インターネットの技術的発展・商用化とともに，サイバースペースを利用した社会経済活動が活発化し，重要インフラ[1] をサポートするシステムもインターネットに接続された結果, インターネット無しでは日常生活が送れないまでになっている. 1990 年代半ばの商用化から 10 年ほどで，インターネットの自律・分散システムとしての利点が明確になり，伝統的な階層システムとしての電話ネットワークに取って代わったが，同時にその便利さはセキュリティ上の脆弱性と表裏一体であることも，明らかになった.

インターネット上では電話ネットワークとは異なり，大量の情報が流通するとともに蓄積されている. この情報の中には，企業や政府部門等の機密情報や個人データが含まれており，サイバー攻撃者はインターネット・システムおよび情報の機密性・完全性・可用性に対する攻撃を行なっている. 加えて，継続的なサービス提供が求められる重要インフラへのサイバー攻撃も顕在化して，経済社会活動や安全保障上の重大な脅威になりつつある[2].

実は，蓄積される情報の中には，あらゆるトランザクションに関するメタデータも含まれているので, これを活用すれば攻撃に対処することが理論上は可能である. しかし，インターネットはもともとベスト・エフォートを前提にした多数の「自律システム（AS = autonomous system）」間の相互接続であるため，統一的な仕様に基づくセキュリティ対策を義務付けることは，原理的に自己矛盾になり，次節で述べるように攻撃優位となっている.

システム全体を通じたセキュリティ・レベルの向上は，電話システムとは対照的に AS 個々の努力に期待するのが基本である（田川 [2013]）[3]. もちろん，個々の努力の総和が統一的な仕様に基づくセキュリティ確保策を上回ることは理論上あり得るが，現代の深刻なインシデント（事故）は故意によるもので，攻撃者は最も脆

[1] 国民生活に不可欠なサービスを提供する基盤となる，電力・交通・通信などのインフラストラクチャのうち，サイバー攻撃から優先的に守るべきものとして国が指定する. わが国では 14 種類のインフラが指定されている.

[2] 2018 年 9 月の地震によって北海道全域が停電して，社会経済活動に大きな悪影響が発生した. また 2019 年 9 月の台風 15 号によって，千葉県を中心に多くの地域で停電が発生して，これが通信の途絶などにも波及して，日常生活に大きな悪影響が生じた. これらの事象をみると，電力に対するサイバー攻撃によって停電が発生すれば，幅広い分野でいかに大きな被害が生ずるかは容易に想像できる.

[3] Internet とは文字通り inter-network（ネットワークのネットワーク）であるから，ネットワーク全体の管理者はおらず，意思決定は全員参加に近いマルチ・ステークホルダー・プロセス，つまり RFC（Request for Comment）などによる多様な参加者の自主的貢献に基づいている.

弱な対象を狙ってくるので，実際上不可能に近い[4] ．

20 世紀におけるセキュリティ・インシデントは，ハッカーと称する個人の自己顕示的行動が多かったため，深刻な事態を招くことは稀であった．しかし 21 世紀に入ると，それらは情報窃取や詐欺等の犯罪と組み合わされて（金儲けというインセンティブを得て），組織化されたサイバー攻撃に転じた．しかも，国家の関与が疑われるような事例も多く発生している．

1.2 サイバー攻撃における攻撃者優位とサイバーセキュリティ対策の課題

サイバー攻撃においては，攻撃側と防御側の間に大きな非対称性があって，基本的に攻撃者が優位・防御側が不利な状況にある（林 [2014]，田川・林 [2017]）．表 1 によれば，評価基準の 8 点のすべてで攻撃側が優位な状況にあるが，中でも ⑧ の行為者の特定（attribution の解明）の難しさが，防御側にとって最大のネックではないかと思われる．

表 1．サイバー攻撃と防御における 8 つの非対称

評価基準	攻撃	防御
① 攻撃の成否	1 点突破でも成功（攻撃側の自己満足だけでなく，事後の攻撃用の踏み台ができる）	100%守れなければ失敗
② 手段の利用可能性	入手容易	入手可能だが不完全（後手に回る）
③ 組織・要員	非政府組織・準政府組織（テロ集団を含む）・Hacktivist などの個人	正規組織（軍・民それぞれ）
④ 予備要員	多数の志願者	正規組織内で指名・訓練
⑤ 国際連携	緩やかな連携（アノニマスが典型）	国家間の任意の協力
⑥ 国家の潜在的支援	その疑いが濃厚	支援は可能だが，手段は国際法遵守のため限定的
⑦ CPU パワーと制御	C&C サーバのコントロールで無限に近いパワーを活用	セキュア環境下での限定的パワー
⑧ 行為者の特定	暗号や TOR （The Onion Router）などによる匿名化が容易	Attribution を特定するには組織と要員が必要

サイバーインシデントの範囲拡大と深刻化の状況のなかで，攻撃者優位の状況を少しでも改善するために，サイバーセキュリティ対策の強化が求められるが，そこには以下のような課題がある．

(1) 防御力の強化の観点から

・SOC（Security Operation Center）などによるオンライン監視によって，サイバー攻撃の検知，被害の拡大防止，原因追及，被害からの復旧，再発防止策の

[4] Varian [2004] によれば，セキュリティの攻防は total effort (全員参加の攻防)，best shot（トップガン同士の攻防）, weakest link（最弱点をめぐる攻防）の三種が代表例とされるが，攻撃が長期的に続くようなケースでは，最後のものが決定的であろう．

実行など監視・解析力の強化
・防御力を高めるための，サイバー攻撃に関する情報共有の仕組みの整備
・近年取組が強化されつつあるサプライ・チェーン対策[5]，セキュリティ・バイ・デザインの強化

(2) 抑止力強化の観点から
・attribution 解明力の強化
・ACD （Active Cyber Defense） による反撃技術力の強化・制度面の整備（林・田川 [2018]）.

前述のような「攻撃者優位」の非対称状況の中で，これらの施策を遂行するには困難が伴ったが，2010 年代に米国を中心にした懸命の努力で，攻撃者を特定する点（いわゆる attribution）で大幅な改善が見られた．その際，最も有力な証拠となったのが，インターネット・サービス・プロバイダ（以下，ISP と呼ぶ）やプラットフォーマ（以下，PF と呼ぶ）の手許に残された膨大な接続履歴（ログ）である．

1.3 ログ[6]の知得･利用の有用性[7]

前節で提起した課題を解決するためには，ログの知得・利用が有効であるとされている．

電話システムとは異なり，インターネットでは，すべての履歴が，ログとして一定期間記録される．このうち何らかの形で「広義の通信」に関係するログは，西欧先進諸国では「通信の秘密」として保護される．ただし，正当なログ知得者が障害復旧等のために「自己利用」することは認められているし，重大犯罪捜査や安全保障等の観点で必要があれば，法に定められた手続きに従って例外的に「公益利用」できるようになっている．

しかし，これらの例外措置は，厳密な手続きを定め十分なモニタリング（監督）のもとに実行しないと，深刻な人権侵害につながりかねない．そのため西欧先進諸国では，「通信の秘密」保護と，その例外措置との間の，価値のバランスを模索する努力が続いている．このバランス論は「公益利用」の場合に，最も顕著に現れる．

このように問題を孕みながらも，ログの活用に期待するのは何故だろうか？ 具体例として，防御側の最大のネックである attribution（行為者の特定）の問題（特にテロと組織犯罪捜査の場合）について，考えてみよう．

まず第 1 に，攻撃者の立場から見ると，「通信の内容」そのもの（パケットでいえば主としてペイロードの部分[8]）を傍受されることは避けたいので，この部分は暗号

[5] サプライ・チェーン対策の強化は，注 6 の Varian のいう weakest link 対策としての性格を有している．

[6] ログという語は，コンピュータの世界では常用されているが，情報を一定の形式で（時系列で）記録したデータのことで，パソコンなどの操作や AS 内・AS 間のイベントの証拠として残された記録，という広い意味がある．本稿では，パソコンの操作などのローカル（stand alone）処理を除き，広義の通信に伴う履歴をすべて含むものと理解しておきたい．

[7] セキュリティ監査の世界では，ログの証拠能力を厳密に検討する必要があることから，ログ＝証跡と短絡的に結びつけることを避ける傾向がある（佐藤(慶) [2011]）．法学の世界でも同様の配慮は必要であるが，本稿では「分かりやすさ」を重視し，厳密性は犠牲にしている．

[8] インターネットのパケットは，通信制御に用いられるヘッダーと，運ばれる通信内容であるペイロードの 2 つの部分からなる．

化するか偽装することが多い．しかし，ヘッダーの部分に手を加えたのでは目的の相手に届かない場合があるので，この部分の暗号化や偽装には限界がある．発信 ID や経由サーバは偽装できても，着信 ID などある程度の情報はサーバに，つまり ISP や PF に渡さざるを得ない．防御対策を考える側からすれば，残ったログから攻撃の実態に近づく手掛かりを得ようとするのは，当然である．

第 2 の理由は，攻撃が個人ベースではなく組織的に行なわれるようになったので，攻撃側からするとメンバー間の密な連絡が必要になり，防御側からすると，この密なコミュニケーションを探知することができれば，「事前抑止に近づき得る」という期待が生ずることである．予めメンバーの範囲と通信手段を特定できていれば，このメンバー間の通信量が急増しただけでも攻撃が近づいた予兆になり得るし，ネットワーク分析の手法が進歩したことで，メンバー間の近接度や役割分担が推定されることもある．

第 3 の理由は，通信内容よりもログの方がプロファイリングに向いている点である．確かに精度の点からすれば，通信内容が傍受できれば攻撃プランをより正確に把握できるかもしれない．しかし攻撃側がインターネットを自在に利用し「なりすまし」が常態化した現在では，技術的に取得が困難で不定形な通信内容を分析するよりも，取得が容易で定型化されたログを大量処理する方が，攻撃者のあぶり出し（プロファイリング）に適している．このような理由から，ログに対する注目度が上がっているのである．

ところでログは，「通信の秘密」に該当する情報またはプライバシー情報[9]であるため，わが国の伝統では秘匿すべき対象であって，これを利用する側面については深く検討する機会が少なかった．しかし，サイバー攻撃が激化した現状では，守秘義務を全うするだけではなく，「秘匿しつつも利用する」プロセスを明確にし，更に守秘の手続きを厳密にする必要があるものと考えられる．

2 「通信の秘密」の伝統的解釈

2.1 憲法における「通信の秘密」

具体的な議論に入る前に，わが国の「通信の秘密」の保護に関連する規定を，改めて概観しておこう．まず「通信の秘密」は，国の最高法規である憲法によって守られている（表 2.）．直接的に言及しているのは 21 条 2 項後段であり，これを具体化する形で後述の電気通信事業法等における「通信の秘密」保護の規定が定められている[10]．

「通信の秘密」の保護法益は，プライバシーを根拠にするという説が有力であり，その点では憲法 13 条が関係する．また，通信は「言論」という形式の情報が流通する 1 つの過程であり，その秘密の保持は広義の「言論の自由」を担保する機能を持つため，21 条1項や

[9] 通信事業者間の論議では，後述するように通信内容とメタデータ（コミュニケーションデータ，通信の構成要素）の用語で区分するのが通例だが，ここでは AS 一般を含めた広い議論をするため，ログの語を用いた．結果的に，メタデータとログとは同じ意味で用いていると理解いただきたい．

[10] より厳密には，憲法の精神が有線電気通信法・電波法の「通信の秘密」保護の規定に生かされ，それを受けて電気通信事業法にも，同様の規定が置かれている．

2 項前段も関係してくる. 更に,「通信の秘密」が侵害されるという事態を回避あるいは最小化することは, 秘密を担保する有力な手段であることから, 35 条の適用もあるとするのが通説である(井上 [1997]).

もっとも, こうしたまとめ方には, ① 個人間の通信(一種の C to C)よりも組織間(B to B)や組織対個人(B to C)の通信が多い現状では, 法人の「通信の秘密」も含めて, その根拠がプライバシーだとする議論には違和感がある(林 [2013]), ② インターネットでは「公然性を有する通信」という, 放送類似のサービスが一般化しており,「(通信の秘密の適用を受ける)狭義の通信とは何か」自体が問題になっている(田川 [2013]), ③ 13 条と 21 条は実体規定であるのに対して, 35 条は手続き規定であり別個に議論すべきではないか, といった論点が残されている[11].

表 2. 憲法における「通信の秘密」関連規定

第 13 条　すべて国民は，個人として尊重される．生命，自由及び幸福追求に対する国民の権利については，公共の福祉に反しない限り，立法その他の国政の上で，最大の尊重を必要とする．
第 21 条　集会，結社及び言論，出版その他一切の表現の自由は，これを保障する． 2 検閲は，これをしてはならない．通信の秘密は，これを侵してはならない．
第 35 条　何人も，その住居，書類及び所持品について，侵入，捜索及び押収を受けることのない権利は，第 33 条の場合を除いては，正当な理由に基いて発せられ，且つ捜索する場所及び押収する物を明示する令状がなければ，侵されない． 2 捜索又は押収は，権限を有する司法官憲が発する各別の令状により，これを行ふ．

2.2 電気通信事業法における「通信の秘密」

電気通信事業法は事業者に対する規律を定める，いわゆる「業法」であるが，そこにおいて「通信の秘密」の保護は，表 3 のように規定されている．

まず一般的規定として，検閲の禁止，秘密の保護，利用の公平の 3 種の規定がある．通常「通信の秘密」といえば，4 条だけと考えられているが，実は 3 条や 6 条も一定の関係性を有することが，後述のいわゆる「漫画村事件」(3.2 節参照) で明らかになったことから，三者を一体として論ずる必要がある．

また 4 条 1 項の「通信の秘密」を侵した場合に刑罰を課す規定が 179 条にあり，1 項では「電気通信事業者の取扱中に係る通信（中略）の秘密を侵した者は，2 年以下の懲役又は 100 万円以下の罰金に処する.」となっているが，2 項において「電気通信事業に従事する者が前項の行為をしたときは，3 年以下の懲役または 200 万円以下の罰金に処する.」となっていて，電気通信事業の従事者が「通信の秘密」を侵した場合には，刑罰が加重されている．

表 3. 電気通信事業法における「検閲の禁止」「通信の秘密」「利用の公平」「侵害への刑罰」

[11] 海野 [2019] は，GPS 捜査を念頭に「監視型情報収集」という新しいタイプの捜査手段が登場したが，それを「強制処分」と位置づけ，35 条の適用を前提に「自己情報コントロール権」からさらに進んだ「私的領域が確保される権利」を主張している．

（検閲の禁止）
第 3 条　電気通信事業者の取扱中に係る通信は，検閲してはならない．
（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．
（利用の公平）
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 179 条　電気通信事業者の取扱中に係る通信（第 164 条第 3 項に規定する通信を含む.）の秘密を侵した者は，2 年以下の懲役又は 100 万円以下の罰金に処する．
2　電気通信事業に従事する者が前項の行為をしたときは，3 年以下の懲役又は 200 万円以下の罰金に処する．
3　前 2 項の未遂罪は，罰する．

2.3 伝統的な解釈における 1 原則と 3 要素[12]

「通信の秘密」の法解釈の大前提になっている基本原則は，表 3 の諸規定の背景にあると思われる，「電気通信事業者は通信には手を触れてはならない」(hands-off) という理念である．これは電気通信事業法 6 条と対をなすものであるし，伝統的なコモン・キャリアの原則として国際的にも常識とされてきた[13]．わが国において，この原則に沿った判例もある[14]．

また電話時代の電電公社社内では「通信の秘密」の保護は「顧客から預かった通信を原状のまま安全に届ける」というコモン・キャリアの使命に直結するものであり，「検閲の禁止」と同様に絶対的なものであるとの認識が浸透していた．そして，こうした認識を基礎にして，以下の 3 つの要素を中心とした法解釈が常識化していた．

1）電気通信事業法 3 条の「検閲の禁止」と 4 条の「通信の秘密」の関係については，具体的事案が発生しなかったこともあって，いままであまり議論されなか

[12] この概念は，共著者が，林・田川 [2019] で提唱したものである．
[13] 電気通信事業の監督機関の国際機関である ITU（International Telecommunication Union）は，hand-off を貫くためかインターネットを所掌することをためらいがちであったが，今世紀に入ってから態度を改めた．しかし，それが逆にコンテンツ規制にも及ぶのではないかとの懸念も生んでいるため，「インターネット非規制」を貫きたい米国は，ITU と疎遠になっている．
[14] 地裁レベルの判決ではあるが，東西 NTT が脅迫的内容の電報の受付・配達を差し止める条理上の作為義務を負うか否かが争われた事件において，「電気通信事業者は,利用者間で通信が行われるに際し，あくまでも物理的な通信伝達の媒体ないし手段として，発信者から発信された通信内容をそのまま受信者に伝達することが，その提供する役務の内容として予定されて」いるとして，差し止めは「公共的電気通信事業者としての職務の性質からして許されない違法行為」であるとされた（大阪地判平成 16.7.7 判時 1882 号 87 頁）．この判決では，電気通信事業者が通信内容に関与することが明確に否定されている．

った[15],

2) 通信当事者以外の第三者が「通信の秘密」を侵す行為として，知得（積極的に通信の秘密を知ろうとする意思のもとで知得する行為），窃用（発信者または受信者の意思に反して利用する行為），漏示（通信当事者以外の第三者が知り得る状態におく行為）の 3 つが含まれるが，この 3 つを区分しつつも，知得を起点とする一連のものと理解する（例えば，多賀谷ほか [2008]）.

3) 通信内容とログの保護レベルを同じと考える.

3 伝統的な法解釈の変質と見直し

3.1 Hands-off 原則の変質

電話時代における「通信の秘密」の厳格な運用については，故ないことではない．離れた場所にいる当事者が通信する場合に，通信を媒介する事業者がその通信を監視しているとすれば，当事者が安心して通信をすることができないからである．この故に注 14 の判例で見たように，電気通信事業者は他人から預かった通信をそのまま運ぶことがその役割であるとして，預かった通信からの hands-off が求められてきた．これが電気通信事業者に課された，本来的な「通信の秘密」遵守の原点である.

電話利用においてはこの hands-off 原則が厳格に守られていたが，インターネット利用では，電気通信事業者が「通信の秘密」の保護の制限に関与を求められる（または認められる）事例が増加している.「通信の秘密」の保護を制限することができるのは，通信当事者の有効な（真性の）同意がある場合と，違法性阻却事由[16] が認められる場合の 2 つとされてきた（別の見方については，4.3 節で紹介する）.

どのような同意であれば有効な同意と言えるのか，またどのような事例に対して違法性阻却事由が認められるのかは，「通信の秘密」の保護法益と「通信の秘密」の保護の制限理由（法益）を比較して判断されていて，これまでに数多くの議論が積み重ねられている.

電気通信事業者が hands-off 原則から離れて，「通信の秘密」の保護の制限に関与する理由は，インターネット上を流通し蓄積されている，いわゆる「違法・有害情報[17]」等に対処するための，いわば「媒介者の責務」に基づく場合と，インターネット・サービスの安定的提供の必要性に基づく場合の 2 つがある（林・田川 [2018]）.

ただし，電気通信事業者が「通信の秘密」の保護を制限する行為を行なうには，相応の法的根拠が必要である．この根拠としては，表 4 に掲げる法律や事業者団体

[15] 憲法学者の間では，検閲の禁止は例外が認められない絶対的なものと理解され，判例もそれを支持している（最大判 1984 年 12 月 12 日民集 38 巻 12 号 1308 頁［税関検査事件］など）．これに対して「通信の秘密」の保護は，例外があり得る相対的なものだが，現場実務ではその差が意識されなかった.

[16] 違法性阻却事由としては，刑法 35 条の正当行為，36 条の正当防衛，37 条の緊急避難がある.

[17] 違法情報と有害情報への対応は当然異なってしかるべきだし，後者の場合は「何が有害であるか」について疑義が生ずる余地がある．しかし，ここでこの論点に深入りすることはできないので，一般の用法に従って「違法・有害情」とひとまとめにしておく.

が自主的に定めるガイドラインがある．いずれの場合も，電話中心の時代には考えられなかったほど幅広く通信事業者の関与が認められており，インターネット利用に関しては，通信事業者の hands-off 原則は，既に変質していると言って良い．

表 4．電気通信事業者が「通信の秘密」の保護を制限する根拠規定

	違法・有害情報等への対策 （媒介者の責務）	インターネット・サービスの安定的提供
法律	プロバイダ責任制限法 青少年インターネット利用環境法	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）
ガイドライン	インターネット上の自殺予告事案への対応に関するガイドライン プロバイダ責任制限法発信者情報開示関係ガイドライン	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 帯域制御の運用基準に関するガイドライン

注 1：迷惑メールがインターネット・トラフィックの大きな割合を占めて，インターネット・サービスの安定的提供に悪影響があるので，迷惑メール防止法 11 条において，電気通信事業者に迷惑メールの取扱い拒否が認められている．またこの取扱い拒否には受信者の望まない e-mail の送信を防ぐという個人的法益もある．
注 2：この他，児童ポルノについてブロッキングが行なわれているが，ガイドラインが公表されていないので，この表には含まれていない．その根拠は緊急避難であるとされるが，疑念も呈されている．

3.2 「検閲の禁止」（事業法 3 条）と「通信の秘密」（同 4 条）の関係

いわゆる「漫画村事件」を契機に，2018 年 6 月から 10 月にかけて 9 回開催された「知的財産戦略本部検証・評価・企画委員会 インターネット上の海賊版対策に関する検討会議」においては，著作権侵害サイトのブロッキングに関して，「通信の秘密」の保護を制限することになるとして慎重ないし否定的な意見が出され，この方式の実施が見送りになった．

この検討会議においては，ブロッキングの問題を「検閲の禁止」であるとする議論が一部[18] ではみられたものの，活発に議論されたというよりも背後に退いていたように考えられる．これは本問題が，「通信の秘密」の厳格解釈の伝統の下で，そもそも認められるのか，という問題設定からスタートしたことも，影響しているものと考えられる．

しかし海賊版のブロッキング問題は，「通信の秘密」の問題である以前に，精神的自由権である「表現の自由」に関わる問題であり（成原 [2018b]），表現の事前抑制である「検閲の禁止」の問題としても，論議すべきではないかと考えられる．例えば，伊藤・前田 [2018] は，「通信の秘密」の側面から見た優れた分析であり，共著者が後述の「知得・窃用・漏示」をアンバンドルするとの着想を得る上で有益であ

[18] 検討会議においては，主として「通信の秘密」から見たブロッキングが検討されているが，宍戸 [2018] は「行政機関のよる（ブロッキングの）判断は，検閲禁止（憲法 21 条 2 項）の趣旨から許されないと解される」また民間団体によるブロッキングの判断についても「私的な団体の判断に，当該団体の構成員ではない利用者一般の知る権利や通信の秘密を制約する法的拘束力を付与することが許されるか，結局のところ，検閲と同じ問題が生ずるおそれ」があると述べており，ブロッキングを検閲の問題としても論じている．

ったが[19],「検閲の禁止」に触れるところがなかったのは意外であった[20].

もっとも「検閲」は公権力の行為であるが，児童ポルノのブロッキングの場合には，いわば「私的検閲」として行なわれており，憲法の「私人間効力」の議論を避けることができない. その際には, 基本的人権を制約するには法律によるべきこと，またその法律の合憲性が認められることが原則である．またガイドラインも公表されているわけではないことなど，ソフトローの有効性についてどう考えるかも問題になるように考えられる.

このような指摘は,「通信の秘密」の保護を制限する場合にも問題となるように思われ，両者に共通項があることを暗示している．いずれにせよ，電気通信事業法 3 条と 4 条の関係は，後述のように従来あまり議論されておらず曖昧さを残しているが,「媒介者の責務」に基づく「通信の秘密」の保護の制限の問題を通じて，今後この両者の関係などの法解釈について検討が深まることが期待される.

3.3 知得・窃用・漏示の区分

「通信の秘密を侵す」態様として,「知得・窃用・漏示」の 3 つがあるとの解釈は定着しているものの，この 3 つの区分についての議論はあまり行なわれていない. しかし現実問題として, 電気通信事業者には自らの業務遂行の必要性に基づき知得・利用する場合があり，この行為は必要な限度で正当業務行為として違法性阻却事由があると認められている.

ただし，業務遂行上の必要性がなく知得した場合や，正当業務行為として知得した情報の管理責任を果たさず窃用・漏示した場合には,「通信の秘密を侵す」行為に該当する．このため，知得と窃用，漏示は解釈上明確に区分して,「通信の秘密を侵す」行為の判断を行なわなければならない.

従って，電気通信事業者が自らの業務遂行上の必要性に基づき知得する行為または「媒介者の責務」として知得する行為については，一般人の知得と区分して，法的にもより明確な形で規律する必要があると考えられる．この点は，無線通信の場合に知得自体は処罰されないが，窃用・漏示した場合に処罰の対象になることを参照すれば，納得できるだろう（電波法 109 条参照）.

またこの区分は，電気通信事業法 4 条 1 項の「通信の秘密」と 2 項の「他人の秘密」の規定が置かれた理由にも関係すると思われるが，共著者のたびたびの指摘にもかかわらず，そのような議論が盛り上がることは無く，両者は解釈上ほぼ未分離の状態にある[21].

---

[19] 伊藤・前田 [2018] の立論には，従来の通信の秘密解釈にはない新しい視点が盛り込まれているが，仮に DNS サーバとのやり取りは「他人の通信の媒介」（事業法 2 条三号前段）ではないとする説を受け入れるにしても，なお「他人の通信の用に供する」（同条三号後段）ものであるとする視点を排除できないので，結論を急ぎ過ぎの嫌いがあると思われる.

[20] 著作権制度が「言論の自由」と関わりを持つことについて，憲法学者が所与としてきたことに警鐘を鳴らした点において，林 [2005] が幾分かの貢献をしたのではないかと密かに誇りにしている．この点に関する憲法学者による分析としては，長谷部 [2012] を参照.

[21] 電気通信事業法 4 条の 1 項と 2 項の解釈については，林・田川 [2018], pp. 51～53 参照.

3.4 通信内容とログの区分

電気通信事業法 4 条では,「通信の秘密を侵してはならない」と規定されていて, 法解釈上「通信の秘密」の対象は通信内容とログの両方であるとされている[22].

わが国においてログを「通信の秘密」の保護対象とした理由は,「これらの事項が知られることによって通信の意味内容が推知される」ためというのが通説である. しかし, 今日のサイバーセキュリティ対策におけるログの活用は, 通信内容を推知するために利用するわけではなく, サイバー攻撃に対して identify, protect, detect, respond, recover[23] するために用いられる. 従って, 少なくともサイバーセキュリティにおいては, ログを保護対象とする通説とログの知得・利用の実態は異なっている.

なお, ログの扱いが「通信内容」の扱いと異なっているし, 異なるべきであるとするのは先進諸国に共通の理解である. 例えば, 米国の ECPA (Electronic Communications Privacy Act of 1986 : 電子プライバシー法)では,「通信内容（content information）と通信内容以外の通信に関する情報（non-content information)」が区分されていて,「通信内容に関しては, その取得についてとりわけ厳格な手続きおよび要件が要求されている」. [24] [25]

また英国の IPA（Investigatory Powers Act）2016 では, 2 編で通信内容に関する特定通信傍受が, 6 編 1 章でバルク通信傍受が, 司法コミッショナーの同意を条件として, 国務大臣が発出する令状で認められている. 一方コミュニケーション・データ（本稿でのログに相当）については, 3 編で司法コミッショナーの同意を得たうえで, 取得申請機関の指定上級者による許可によって取得が認められていて, ログの取得が通信内容の取得よりも要件が緩和されている.

ただし, バルク取得については, 6 編 2 章で司法コミッショナーの同意を条件として, 国務大臣の発出する令状が必要となっている[26]. また, バルク令状については, 通信傍受とコミュニケーションデータ知得のいずれの場合も, インテリジェンス機関（GCHQ = 政府通信本部, SS = 内務省保安局, SIS = 秘密情報部）に対してのみ認められている.

このように現在の法制度では, 通信内容の知得に対してログの知得よりも厳格な要件が課されているが, 1.3 節で述べたように, サイバーセキュリティ分野, とりわけ attribution の解明にとっては, 通信内容よりもむしろログの知得・利用の有効性が高くなっており, 通信内容とログの区分を重視する意味合いが薄らいでいるのが

---

[22] 「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をなすものではないが, 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. 電気通信関係法コンメンタール編集委員会 [1973], p. 39.

[23] この 5 つの用語は, 5.4 節にある NIST の Security Framework にある用語.

[24] 「インターネット時代の『通信の秘密』各国比較」情報セキュリティ大学院大学「インターネットと通信の秘密」研究会 第 2 期研究会報告書（2014 年), pp. 23～24.

[25] 米国では, 愛国者法 215 条によりメタデータの bulk collection（大量収集）が行なわれてきたが, 2015 年の US A Freedom Act 以降は, 裁判所の命令に基づいて特定の対象者の通信についてのみ, メタデータの収集が限定的に認められるようになっている.

[26] IPA2016 の内容については, 情報セキュリティ大学院大学[2017]を参照.

現状である.

この現状を受けて，米国では（現行規定で通信内容の取得について，より厳格な手続きを要求するのは）「通信の内容以外の情報を蓄積して分析することによって，個人のプライバシーに重大な影響が及ぶことが指摘されており，インターネット時代においてはかかる区分はもはや意味をなさなくなっている 」との指摘もあり[27]，ECPA の改正論議も行なわれているようである[28].

3.5 分節化（アンバンドル）の提案

以上検討してきたことから本稿では，従来明確に区分されていなかった「通信の秘密」の諸要素の「分節化（アンバンドル）」を徹底して，インターネット利用にふさわしい法解釈に見直すことを提唱したい．その要点は，以下の 6 点にわたるアンバンドルである.

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（通信履歴）」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，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「ユーザの同意」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「バルクデータ」の扱いを別にする.

その上で本稿の焦点は，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を念頭に，ログの知得・利用を違法・有害情報等に対する「違法性阻却」とは「別建て」とする案を検討する。併せて ④ ⑤ においては，「ログの知得・利用・廃棄」の可能性と，濫用を防止する制度的な仕組みを探る．そこで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適正運用をどのように担保するかである.

なお残念ながら ⑥ においては，さし向き特定データを念頭に置き，バルクデータは今後の課題とせざるを得なかった. これはわが国のインシデント情報の共有が，現状では官民一体型の段階にあり，政府対応力を強化した官民一体型を将来の課題としていることに対応している（この点は，5.2 節で詳説する）.

---

[27] 前掲注 26 文献，pp. 24～25.

[28] もともと，ログの取得・利用に関する規律が，「通信の内容」に比して「より緩やか」でよいかというと，その理論的根拠は必ずしも明確ではない.「第三者法理」により「相手を信頼して情報を提供した場合は，プライバシーの合理的期待は生じない」とする米国の法理は明確だが，現在も維持されているかどうかは議論がある（Thompson [2014]などを参照）. PNR（Passenger Name Record）のように航空機のハイジャック対策として欠かせない情報を，関係機関が共有することについて反対はないが，これが広義のコミュニケーションにおける「通信内容」に当たるのか，ログに当たるのかという議論はなされていない. そうした business record へのアクセスがどこまで認められるべきかの一般原則はなく，アド・ホックな議論に終始している . https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en

4 電気通信事業者による通信内容とログの知得・利用事例と根拠

4.1 通信内容とログの知得の現状

表 4 において，電気通信事業者による「通信の秘密」保護の制限が求められ（違法・有害情報等に関する媒介者の責務に基づく制限行為），あるいは認められる（インターネット・サービスの安定的提供のための制限行為）事例と根拠を示した．ここでは更に進んで，知得・利用する情報の区分（通信内容かログか），知得範囲を特定して知得するログ（特定データ）か範囲を特定しないで悉皆的に知得するログ（バルクデータ[29]） かの区分毎に，現状でどの程度の知得・活用がなされているかを調査した結果，表 5-1 及び 5-2 [30] を得た．

なお，国家権力が「通信の秘密」の保護を制限する典型例として，通信傍受法がある．この法律による傍受には裁判所の発出する令状が必要になるのに対して，本章で検討する事業者が関与するケースには，令状は必要とされていない．

表 5-1 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「媒介者の責務」を果たす場合）

事例	① 発信者情報開示	② 青少年閲覧防止措置	③ 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	青少年インターネット利用環境整備法 21 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	青少年の健全な育成環境の実現	人命保護
知得内容	特定の発信者情報（特定データ）	通信経路上でバルクデータを知得して，有害サイトのリストに基づき，送信防止サイトを抽出	特定データ

表 5-2 電気通信事業者による通信内容とログの知得・利用事例（インターネット・サービスの安定的提供の場合）

事例	④ 迷惑メールの取扱い拒否	⑤ サイバー攻撃に対する対抗措置	⑥ 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	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	帯域制御の運用基準に関するガイドライン

[29] バルクデータの知得というのは，知得対象データを特定しないで，すべての流通・蓄積データを知得することを意味する．米国オバマ大統領が 2014 年 1 月に発出した PPD (Presidential Policy Directive：大統領政策指令) -28 号 2 条注 5 では，バルクデータは以下のように説明されている．“Reference to signals intelligence collected in **bulk** mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g. specific identifiers, selection terms, etc.). 下線は付加（林・田川 [2016]）．

[30] 表 5-1 および表 5-2 の知得内容の記述については，小山覚エヌ・エフ・ラボラトリーズ社長にご教示いただいた．ここに謝意を表したい．

	法律)	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-mail の送信防止	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
知得内容	メールサーバ上でバルクデータを知得して，迷惑メールのリストに基づき，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，帯域制御を行なう

ここで，2 点注意すべき点がある．

第 1 点として，ソフトローであるガイドライン（事業者団体が制定者）は，制定団体自体が「本ガイドラインはあくまでも業界における解釈に過ぎず，法的な効果があるものではありませんが，通信の秘密に関わる解釈指針として，電気通信事業者及び関係者による法的判断の解釈の参考として参照されることを期待するものです.」[31] と述べているように，あくまで法的解釈の参考資料である．もっともこれらのガイドラインの基本的な内容は，総務省の研究会等の議論を反映しているので，いわば「共同規制[32]」的な手法が取られているものとも言える．

しかし，国民の権利を制限する根拠が法律ではなく，業界団体の作成するガイドラインであることの正当性については疑義もある[33]．法律に規定しなくとも，少なくとも主管官庁である総務省の告示とすることも，検討する必要があるように思われる[34]．非政府機関のガイドラインである限り，法的な不安定性が避けられないからである．特に「違法性が阻却されなければ刑事罰を受ける」という状態は，ログの知得・利用が必要な場合も「控え目に対応する」傾向を生んでいる．

第 2 点として，上記の事例をみると，違法・有害情報等の流通対策およびインター―ネット・サービスの安定的提供のために，既にログの知得・利用が広範に行なわれている現状にあることが分かる．しかしログは，「通信の秘密」に該当する情報またはプライバシー情報であるので，知得段階だけではなく，保存・利用（公開）・廃棄段階を含めた「情報のライフ・サイクル全体」における安全管理や廃棄段階での規律（情報保全）も必要になる[35] と考えられる．

[31] 2018 年 11 月の改定（第 5 版）の報道発表資料.

[32] インターネット利用における共同規制について，生貝 [2011] は「効率的かつ実効的なコントロール・ポイントを特定し，それらが行う自主規制に対し一定の公的な働きかけを行うことにより，公私が共同で解決策を管理する政策手法」であると定義している．本稿の場合には，ISP がこの「コントロール・ポイント」に該当する．

[33] 2019 年 4 月に海賊版サイトに対してプロバイダに対してブロッキングを行なうことを政府が要請するとの報道がなされたことに対して，一般財団法人情報法制研究所が政府要請を控えるようにとの緊急提言を行なった．その理由として「緊急避難」の要件充足性に関する疑問，通信の自由を支えるプロバイダに対する不合理な負担とともに，法治国家原理からの逸脱を挙げている．この原理に基づき，「個人の権利を制限し，あるいは義務を課すためには法律（又はその具体的な委任を受けた命令）に基づかなければならない」としている．表 5-1 と 5-2 にみるように，事業者団体が協議して作成したガイドラインによって，通信の秘密の保護の制限が行なわれている現状に，疑問を呈したことになろう．

[34] 因みに，「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」は総務省告示になっている．

[35] 前掲注 34 のガイドラインにおいても，ログの安全管理や保存などについて規定されている．

4.2 「通信の秘密」の保護法益

「通信の秘密」の解釈と運用が憲法の定める理念に即しているか否かを判断するには，保護法益は何かを議論する必要がある．この点に関する憲法学説には，プライバシー保護を重視する説（佐藤(幸) [2011] p.321，長谷部 [2014] p.229，大石・大沢 [2012] p.110 など）[36]，表現の自由との関連を重視する説（阪本 [1995] p.139，渋谷 [2013] pp.412~413 など）[37]，両方であるとする説（長谷部ほか編 [2013] p.263）がある．一見すると解釈が分かれているが，鈴木 [2008]（p.136）によれば表現の自由の 1 つとしての意味を有するとしながらも，私生活・プイバシー保護の一環としての意味を重視しているのが多数説であるとしている[38].

しかし近年有力になっている説として，表現の自由（親密な表現，匿名表現），プライバシー（個人情報の保護との重なり）に加えて，通信の自由または通信制度の保護の 3 つ（宍戸 [2018]）であって，「通信の秘密」の保護は，「その前提となる通信の自由をも保障する規定と解される」との見方（宍戸 [2016] p.216）がある．

また曽我部 [2013] は，「通信事業が自由化された後は，民間の通信サービス利用を公権力に妨げられないという意味での通信の自由は重要な基本権として保障されるべきである.」と述べ，公権力の関与の視点から通信の自由を捉えている．

ここで「通信の自由」という概念が登場したことの意義を考えてみると，プライバシーを確保するとともに，精神的自由権である表現の自由を最大限尊重するという点において従来の通説とさほど変わらないが，その 2 つの価値を実現するには通信システム自体が信頼に値するものであることが前提になっている，との期待感の現れがあると考えられる．

このような考え方は，長年通信ビジネスに従事してきた共著者の感性に合うものであり，電気通信を所管する総務省にも，違和感なく受け入れられるものと思われる．現に同省の「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ」（2014 年 4 月）においては，「通信の秘密は，個人の私生活の自由を保護し，個人生活の安寧を保護する（プライバシー保護）とともに，通信が人間の社会生活にとって必要不可欠なコミュニケーションの手段であることから，憲法上の基本的人権の一つとして憲法第 21 条第 2 項において保護されている.」としている[39].

---

[36] なお長谷部は，「通信の秘密はプライヴァシーの核心部分の一つであり，憲法はこれをとりあげて明文で保障したもの」と述べている．

[37] なお阪本は「通信の秘密」を通信の自由の一環として捉えて，表現の自由との関連を重視している．

[38] 保護法益がプライバシーであるとすると，現在の通信では C2C の通信よりも，B2B あるいは B2C の通信の方が多いので，電気通信の当事者である法人の位置づけが疑問になる．このことに関して，「プライバシーは個人の権利であるが本条（電気通信事業法 4 条）は法人にも適用されることや，罰則の担保があることから，プライバシー権のみでは本条を基礎づけることはできない」との指摘がある．多賀谷ほか [2008] p. 37

[39] また「インターネット上の海賊版サイトへのアクセス抑止方策に関する検討会報告書」（2019 年 8 月）においては，「憲法において通信の秘密を保護する意義は，国民のプライバシーの保護にとどまらず，国民の表現の自由や知る権利を保障すること，さらに国家権力が通信の秘密を侵害しないのみならず，私人による侵害から通信の秘密を保護し，国民が安全・安心に利用できる通信制度を保障することにより，国民の通信の自由を確保することにあると考えられる.」として，電気通信事業法は憲法上の要請を担保するために法律レベルで具体化したものであると述べている．

4.3「通信の秘密」と他の法益との比較較量あるいは相補的理解

違法・有害情報等の対策のために「通信の秘密」の保護を制限することの是非を検討する場合は，前節で検討した通信の秘密の保護法益と，違法・有害情報を流通させないという社会的利益の比較衡量になると考えられる．前者が上回れば「通信の秘密」が優先され，後者が上回れば「通信の秘密」の保護が制限される[40].

一方, 通信の自由のもう一つの意義として, サイバーセキュリティ上の脅威から, 情報および情報ネットワークシステムの機密性・完全性・可用性を守るという視点がある. すでに述べたように, 社会経済活動が多くを依存しているインターネット・サービスの安定的提供を確保するのも，電気通信事業者に期待される責務だからである.

この違法・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」の保護を何らかの形で制限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」の保護法益と他の法益とが「あれかこれか」の関係になるが，後者においては，サイバーセキュリティ対策などを強化して通信の自由を確保することが，むしろ「通信の秘密」の保護を強化することにもなる（両者は相補的である）とも言え，通信の秘密の保護とサイバーセキュリティ対策は対立するものではないと考えられる[41]. 後者にふさわしい用語としては,「通信の自由」というよりも, むしろ「通信の安全」というべきかもしれない.

前節で紹介した「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ」には,「通信が人間の社会生活にとって必要不可欠なコミュニケーションの手段」を守るとの問題意識がみられる．そして，サイバー攻撃等からインターネット・サービスの安定的提供を図るために，通信遮断等のためにログを知得・利用することを想定しているが，プライバシーの問題はあるものの，表現の自由の制限という要素は希薄である.

このように考えてくると，違法・有害情報等の対策のために「通信の秘密」の保護を制限する場合と，インターネット・サービスの安定的提供のために「通信の秘密」の保護を補正（あるいは制限）する場合とでは，議論を切り分けて検討する必

---

[40] 違法有害情報等の対策に電気通信事業者が関与するのは,「媒介者の責務」に基づくものであるが，成原 [2012] はこの責務を国家が間接的に表現の自由を規制する試みとして論じている．媒介者の行為が「代理人による検閲（Censorship by Proxy）に該当する場合があること，また媒介者の行為は可視性が低いこと，媒介者は第三者の表現の自由を保護するインセンティブが少ないこと，疑わしい表現をすべて遮断する」リスクがあることを指摘している．この観点から，現在の違法・有害情報等に関する対策をみると，プロバイダ責任制限法でも，自殺予告事案に関するガイドラインでも，検閲的な要素はない．また青少年インターネット利用環境法 21 条における青少年閲覧防止措置も，プロバイダ（特定サーバ管理者を含む）が自ら情報を探索する必要はなく，青少年有害情報の発信を知ったときに閲覧防止措置をとることになっており，またこの措置は努力義務なので，措置を取らなかった場合に法的責任を問われることはない．このように少なくとも現時点ではプロバイダが「代理人による検閲」を行なうリスクは，限定的ではないかと考えられる.

[41] 多賀谷 [1995] は,「データ通信（共著者注：今日的にはインターネット）においては，通信の秘密は広い意味での通信セキュリティ（同：今日的にはサイバーセキュリティ）の一要素にすぎず，通信の秘密の保護と並んで，通信にエラーのないこと（完全性の要求），（中略）など通信セキュリティの保全が求められる.」と指摘している（pp. 190~206）．この指摘は，インターネットが普及するかなり以前の 1995 年になされたものであり，その先見性に驚かされる.

要があると考えられる[42]. この意味でのアンバンドルは, 過去に検討されたことがないが, サイバーセキュリティ対策を考える上では, 必要な準備作業ではないかと思われる（3.5 節における ③）.

ただし, ログの知得・利用に関するプライバシー保護については, 両者に共通しており, いずれの場合もログが大量に知得・利用されるようになるので, 適正な知得・解析・情報共有・対策への利用・保存・廃棄の各プロセスにおけるルール化は, より一層重要になると考えられる.

4.4 「有効な同意」のあり方

「通信の秘密」を侵害する行為であっても, 通信当事者の有効な同意がある場合, または違法性阻却事由がある場合には, 適法な行為であるとされている.「違法性阻却事由」を広義に解すれば「利用者の同意」もこれに含まれるが, いずれにせよ「有効な同意」を根拠とするログの知得の利用範囲は広い. そこで, どのような場合に「有効な同意」があるといえるのかを考えてみたい.

有効な同意に関する総務省の見方は,「通常は契約約款等に基づいた事前の包括同意のみしかない場合を含まない.」,「具体的には, 通信の秘密の取扱いについての同意であることを本人が認識した上で行なう個別の同意であり, かつ, 画面上での操作や文書による同意など外部的に同意の事実が明確な同意を意味[43]」しているとされる.

この原則に対して, サイバー攻撃に関して設置された一連の研究会においては,「マルウエア配布サイトへのアクセスに対する注意喚起」を行なう場合に, 契約約款等に基づく事前の包括同意であっても, 一定の条件の下においては, 有効な同意ということができないかとの視点から検討が行なわれた.

結論としては ISP が知得する「通信の秘密に該当する情報のうち必要最小限度の事項（アクセス先 IP アドレスまたは URL）のみを機械的・自動的に検知」するもので,「インターネットアクセスサービスの通常の利用者であれば, その限りにおいてこれらの事項が利用されることについて許諾することが想定し得る」場合は, 一定の条件の下で,「有効な同意ということが考えられる[44].」と, 個別かつ明確な同意に対する例外を認めている.

上記の事例は, インターネット・サービスの安定的提供のために, 電気通信事業者が「通信の秘密」の保護の制限を行なう事例である. これに対して, インターネット上の海賊版サイト対策としてのアクセス警告方式[45] についても, 包括的な同

---

[42] 第 3 の類型として「プロバイダ責任（制限）法における発信者情報開示の制度を拡充し, 消費者訴訟をやりやすくする」との日本弁護士会の提案があるが, 米国のディスカバリ制度との対比など論ずべき点が多いので, 別途の機会を得たい.
http://www.soumu.go.jp/main_content/000105851.pdf

[43]「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第三次とりまとめ」2019 年 9 月, p. 10.

[44]「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第一次とりまとめ」2014 年 4 月 pp. 19~21

[45] ユーザの同意に基づき, インターネット接続サービスを提供する電気通信事業者が, ネットワーク上のアクセス先（海賊版サイト以外のサイトへのアクセスも含む.）をチェックし, ユーザによる海賊版サイトへのアクセスを検知した場合に,「本当に海賊版サイトにアクセスしますか？（はい/いいえ）等の警告画面を表示させるなどの仕組みをいう（「インターネット上の海賊版サイトへのア

意によって電気通信事業者が「通信の秘密」の保護の制限を行なうことができるかについて検討が行なわれた.

この検討過程ではユーザに対するアンケート調査が行なわれたが,「アクセス警告方式を実施することに対して，通信の秘密や検閲といった観点から慎重又は否定的な意見が多く提出された」ため,「ユーザの意識・意向を踏まえると，アクセス警告方式の実施について，一般的・類型的に見て，通常のユーザであれば許諾すると想定し得るとはいえないと考えられる」として,「アクセス警告方式の場合には契約約款等による包括同意を有効な同意とみることは困難[46]」であると判断された.

このように,「アクセス警告方式」と「マルウエア配布サイトへのアクセスに対する注意喚起」に関する包括同意について，前者は認められないが，後者は認められると結論が分かれた. 利用者からみて，違法・有害情報等の場合とインターネット・サービスの安定的提供の場合とでは，同じ「通信の秘密」の保護を制限する行為であっても，許容度が異なっているように考えられる.

もっとも，後者の包括同意が認められた事例では，ユーザの意識・意向調査は行なわれていないので確定的なことは言えないが，後者は通信の安全を確保する行為であるのに対して，前者は表現の自由もしくは自分のインターネット利用が監視されている，通信の自由が制限されると受け止められるからであると推測される.

更に言えば，前節で述べたように，違法・有害情報等の対策のためのアクセス抑止方式と，インターネット・サービスの安定的提供とでは,「通信の秘密」の保護法益との関係が異なること（前者は比較較量的＝二者択一的，後者は相補的）が，利用者の意識・意向にも反映されているとも考えられる.

この有効な同意の議論は,「通信の秘密」の保護を制限する行為であっても，通信当事者の有効な同意がある場合には適法な行為となるとの考えが前提になっている. この通信当事者の同意を基礎に適法な行為を判断することに疑問を投げかけているのが，ローレンス・レシグである. その理由として彼は,「ユーザはデータがどう使われるか理解でき」ないからであるとし，むしろ「政策によってデータの適切な用途と不適切な用途の推定を下す」べきであるとしている[47].

また同意（承諾）によって（適法との）法的効果が生ずるとは，必ずしもいえない. 例えば他の法領域を参照してみると，刑法 202 条の自殺関与及び同意殺人の規定や著作権法 59 条の著作者人格権の一身専属性の規定では，当事者が同意（承諾）してもその法的効果は認められておらず，同意（承諾）の有効性が否定されている.

4.5 国際比較による「通信の秘密」の意義再考

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ことや，厳格な解釈が実務上の桎梏となっているケースに重きを置

クセス抑止方策に関する検討会報告書」2019 年 8 月，p.7).

[46] 前掲注 45 の文書, p. 13.

[47] レシグのこの指摘は，多くのネット利用に関して，日常的にワンクリックで利用規約に同意することに関して述べたものであるが,「有効な同意」ではなく「同意の有効性」に疑問を呈しているものと考えられる. 出典 :「ローレンス・レシグに聞く，データ駆動型社会のプライバシー規制」 https://www.technologyreview.jp/s/154785/interview-with-lessig-privacy-regulation-in-the-data-driven-society/

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．それは，2019 年 1 月 23 日付の EU 委員会の日本に関する十分性決定[48] において，EU 側が十分性を認定した大きな理由として,「通信の秘密」の規定に言及していることである[49] [50].

また学界においても，宍戸は,「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[51].」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.

成原［2018a］は「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．従って,「通信の秘密は，我が国特有の『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,「我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,「通信の秘密」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.

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，欧米の法制度と普遍的価値の共有につながるので，サイバーセキュリティに関する国際連携やこ

---

[48] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0419c 参照．十分性決定に関する EU との交渉経過については，堀部 [2019a] [2019b]を参照,

[49] 前掲注 48 の文書の前文(116)，(129)参照.

[50] 今回の ANNEX2 の記述は，日本側が提出した文書に沿った内容であるが，日本には「通信の秘密」の規定があることと，政府アクセスは現在重大犯罪捜査のための通信傍受法だけで，国家安全保障目的の強制力のある情報収集・アクセスは許されていないと述べられている．2016 年 7 月に発効した米国・EU 間のプライバシーシールド交渉では，米国側の政府アクセスの在り方が EU 側の大きな関心事であった．このプライバシーシールドを意識して，十分性認定を得るために，国家安全保障のための法制度がないことを述べたものと想像されるが，今後サイバーセキュリティ対策強化の観点から公権力の関与を強化する法制度の検討が必要になる可能性があり，その検討に際してネガティブな影響を与える懸念がある．なおプライバシーシールドの内容および発効にいたる経過については，林・田川 [2016] pp. 18～20，pp. 25～26 および石井 [2017]「第 4 章第 2 節 セーフハーバー・スキームの見直し」を参照.

[51] 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」

の分野に関する法分野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.

このような理解は，インターネットのガバナンスをめぐる国連の努力を象徴するGGE（Group of Governmental Experts）の会合が，5 次にわたる討論を経ても合意に至らなかったこと[52], その原因は, 国家主権がインターネットのグローバル展開よりも上位にあるべきだとするロシア・中国などと，国境を超える情報の自由な流通に価値があるとする西欧諸国との間の「越えがたい壁」にあることを考えるとき，より一層の意義を見出すことができよう（林 [2017]）.

5 ログの活用と手続的保障の必要性

5.1 違法性阻却のみを根拠にした発想からの脱却

総務省では，電気通信事業におけるサイバー攻撃の拡大・深刻化に対処するために,「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」を設置して,「通信の秘密」の問題を検討してきた．その成果として，2014 年 4 月に「第一次とりまとめ」を，2015 年 9 月に「第二次とりまとめ」を，さらに 2018 年 9 月に「第三次とりまとめ」を公表している.

これらのとりまとめ内容を反映させる形で，前掲の「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」が複数の電気通信事業者団体の協議によって制定・改定されている．ガイドラインの初版は 2007 年，第 2 版は 2011 年であり，2014 年の第 3 版から総務省研究会のとりまとめ結果を反映するようになった．また，2015 年の第 4 版からガイドラインの名称が現在の名称に改められた.

総務省研究会のとりまとめおよびガイドラインにおいては,「通信の秘密」を侵す行為であっても，前述したように「通信当事者の有効な同意に基づく場合又は違法性阻却事由がある場合に限り，通信の秘密の侵害に該当しない[53]」との解釈の下で，有効な同意とはどのような同意なのか，違法性阻却事由が認められる場合が検討されている．特に第三次とりまとめでは，正当業務行為として認められる要件[54] および正当防衛，緊急避難が認められる要件[55] が記載されている.

これらの要件は，新しいサイバー攻撃手法が登場するたびに，総務省の検討会でかなりの時間をかけて詳細な検討が行なわれ,「サイバー攻撃等への対処と通信の秘密」のガイドラインの改定に結実したものである．このプロセスを経る理由は,「通信の秘密」保護の制限を行なう行為に関して，違法性阻却事由の有無を個々に判断

[52] http://www.itresearchart.biz/?p=912
[53] 前掲注 43 の文書，p.10.
[54] 電気通信役務の円滑な提供を果たすという見地からみて，①目的の正当性，②行為の必要性，③手段の相当性が認められる行為については，正当業務行為としてその違法性が阻却される．出典：前掲注 43 の文書，p.11.
[55] 正当防衛として違法性が阻却されるためには，①急迫不正の侵害に対し，②自己又は他人の権利を防衛するために，③やむを得ずした行為である必要がある．緊急避難として違法性が阻却されるためには，①現在の危難を避けるため，②法益の権衡が図られる限りにおいて，③他にとるべき方策なしに（補充性）行った行為である必要がある．出典：前掲注 43 の文書，p.11.

する必要がある，との理解に基づくものであろう．

ここには，私たちが 3.5 節で行なったような分節化（アンバンドル）の発想がないため，サイバーセキュリティ対策としてログを利用する場合は，「通信の秘密」と相補的であるという理解を欠き（3.5 節におけるアンバンドルの ③），違法・有害情報に対処する場合と同様「違法性阻却」を判断基準にしている点が問題である．

また，新たなサイバー攻撃手法が登場してから，詳細な検討を行ったうえで対抗策が認められるまで時間がかかることから，対抗策が後手に回りやすい[56]．加えて，違法性阻却事由があれば適法，なければ事業法 4 条違反で 179 条の罰則適用と正反対の結論になる（刑事罰が科されるので，その差は顕著である！）ため，新たなサイバー攻撃手法に対する対抗措置の合法性について結論が出るまでは，事業者が対抗措置の実行をためらいがちになる[57]．

一方利用者の有効な同意については，4.4 節で述べたように，個別・明確な同意が必要とされるのが原則であるが，サイバー攻撃への適正な対処策を取ることに関しては，この原則を転換して，第一次とりまとめでは，「マルウエア配布サイトへのアクセスに対する注意喚起における有効な同意」の検討の中で，通常の利用者ならば同意することが想定し得るので，オプト・アウトなどの一定の条件[58]のもとで，約款に記載することで良いとの方針が示され，この考え方がその後のとりまとめでも維持されている．

この想定がサイバー攻撃などに関して一般化すれば，新たな攻撃手法に関する対策への判断が早くなり，より抽象度の高い判断枠組みの形成につながる可能性がある（林・田川［2016］）．しかし，そのためにも，3.5 節におけるアンバンドルの ③ を明確に意識すべきではないかと考えられる．

こうした考察を発展させると，サイバー攻撃等に対処のためのログの知得・利用に関しては，他の場合と「別建て」にすることも考えられる．ログを「通信の秘密」の保護対象とする理由が，ログによって通信の意味内容を推知されるためとするのが通説であるところ，サイバー攻撃等への対処のためにログを知得・利用するのは，前述したように通信の意味内容を推知するためではないからである．

これによって，違法性阻却事由があるかどうかをまず研究会で個別に検討して，その後ガイドラインに反映するような現状の方式を避けることができ，新たなサイバー攻撃への対処策が迅速に取れるようになる．ただし，サイバー攻撃等への対処のためのログの知得・利用であっても，プライバシー保護は重要であるので，情報のライフ・サイクル全体を通じた適正な取扱いは不可欠である．

加えて，この迅速なサイバーセキュリティ対策の実行は，サイバー領域が国家安

---

56 サイバーセキュリティ分野のトップガンの一人とされる名和利男氏は，攻撃者の攻撃技術の高度化によって，新たな攻撃手法が開発され，また民間組織が検知或いは識別することが困難なサイバー攻撃が増えている現状に警鐘を鳴らしている．出典：名和利男「サイバー脅威に対する状況認識のために整備すべき態勢と獲得すべき能力」情報法制研究第 3 号，2018 年 5 月号

57 米国ではある行為の適法性が明確ではない場合でも，まず行動して，問題が生ずれば是正するとのリスクテイク型の行動が多いのに対して，日本ではリスク回避型の行動が多いことが，その背景にあると考えられる．

58 同意しない者の利益が侵害されないような態勢を整えこと，一旦同意した後も同意内容を変更できること，同意内容の変更の有無に関らずその他の提供条件が同一であること，といった条件が満たされることが挙げられている．出典：前掲注 44 の文書，pp. 19～21.

全保障の観点からも対策強化[59]が求められている状況にあるだけに，次節に述べる将来形の第 6 段階のあり方をも視野に入れて議論しなければならない.

4 章と本節における考察から，サイバー攻撃等に対処するためのログの知得・利用を，他の場合と「別建て」とすることも考えられると述べた.「別建て」の検討課題としては，どのようなサイバー攻撃等を対象とし，どのような条件の下で「別建て」を認めるか，サイバー攻撃等に対する防御力と抑止力としてどのような手法とレベルまで認めるか，どのような情報共有と情報保全の仕組みを作るか，どのように担当組織を整備するか，技術力・産業力強化策をどう講ずるか，どのような法形式（法律かガイドラインか、現行法改正か新規立法か）とするかなど，法制度設計上は難しい課題が多い.

またサイバー攻撃等による重要インフラの可用性喪失を含む社会経済活動の混乱ないし停滞は，国家安全保障上の重大脅威でもある一方，基本的人権とのバランスをどう取るかが，この法制度設計上の基本的視座である．今後のサイバーセキュリティ上の脅威の変化を把握・予測するなかで，課題の検討が深まっていくことが期待される.

5.2 個別企業によるログの知得・利用から情報共有へ

ところでログを知得し利用する主体は，第一義的には被害を被った私企業などの組織か，当該企業等からセキュリティ確保を依頼されたセキュリティ・ベンダ，クラウドを含めた情報処理事業者，電気通信事業者（ISP を含む）等であろう（以下，これらの事業者を総称して「セキュリティ・ベンダ等」と呼ぶ）. これらの事業者は，一般のユーザに比べればセキュリティに関するリテラシーに富んだ者であるが，それでも単独で悪質な攻撃者に対処できるかというと，心もとない.

それは 1.2 節で述べたように，攻撃者に対して防御側が比較劣位にあるからで，その欠陥を克服する第一歩は「関係者間の情報の共有」であることが，強く意識されている. しかも，それには段階があり，私企業間の相対のものからスタートして，業界全体をカバーするものに発展し，業種を超えて組織化され，やがては官と民の区分をも超えていくものと理解されている. その際, 利用が期待される情報として，上述の各民間事業者が保有するログとともに，政府機関，特にインテリジェンス機関の有する情報の役割が重視されている.

インテリジェンス機能は，人間を対象とする HUMINT（HUMan INTelligence）から始まり, SIGINT（SIGnal INTelligence）, GEOINT（GEOspacial INTelligence）などが分化してきたが, 今日最も注目されているのは, COMINT（COMmunications INTelligence）である．英国において COMINT 機関である GCHQ（Government Communications Headquarters）の内部に NCSC（National Cyber Security Centre）が設置され，英国全体のサイバーセキュリティの司令塔となったことが，それを象徴している.

[59] 新たな防衛分野としてサイバー領域が挙げられていて, この領域のおける今後の防御力および抑止力強化の方針が打ち出されている．出典：「平成 31 年度以降に係る防衛計画の大綱について」平成 30 年 12 月 18 日.

そこでログの知得・利用に関しても，以下のどの段階にあるのか，あるいはあるべきかが重要な論点になろう．

① 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．

② 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．

③ 第 3 段階：民間共有型
JPCIRT/CC（Japan Computer Emergency Response Team Coordination Center）のようなセキュリティ・ベンダではない民間組織が，会員企業からのログを情報共有し，サイバーセキュリティ対策を行なうケース．

④ 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，民間企業とログ情報を共有して，サイバーセキュリティ対策を行なうケース：政府の間接関与．

⑤ 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ログ情報を共有して，サイバーセキュリティ対策を行なうケース：政府の直接関与．

⑥ 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）を行なうケース．

共著者の理解では，わが国の現状は ④ から ⑤ への移行期にあるが，近い将来には ⑥へと移行(あるいは飛躍)することが不可避ではないかと思われる．それは，「現在，そして近い将来に国家主体によるサイバー攻撃が行なわれ，民間の自主的な対応ではそれを防ぐことが出来ない」と考えているからである．

5.3 モデルとしてのサイバーセキュリティ連絡協議会

「攻撃者優位」にあるサイバーセキュリティ対策の第一歩は「情報の共有」であるが，共有に種々の障害があることも，米国の経験から知られている（林・田川 [2018]，永野 [2018]）．この意味で，サイバーセキュリティ基本法を改正して，内閣情報セキュリティセンターが主導する「サイバーセキュリティ協議会」という連絡調整機関が設置されたことは，共有の阻害要因を除去するものとして注目される．

これに先行する形で，総務省は「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（通称 NICT 法）の一部改正法」を成立させた．前段の改正電気通信事業法では，「第 7 節 認定送信型対電気通信サイバー攻撃対処協会（第 126 条の 2～第 116 条の 8)」を新設した[60]．この規定は電気通信事業者による攻撃通信の発生

[60] 「送信型対電気通信設備サイバー攻撃」の定義は，「情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する攻撃のうち，送信先の電気通信設備の機能に障害を与える電気通信の送信（当該電気通信の送信を行なう指令を与える電気通信の送信を含む.）に

の防止を図るために，協会が C&C サーバ等に関する情報を集約し，分析・検証した上で電気通信事業者との間で情報共有を図ろうとするものである．協会が「通信の秘密」に該当する情報を扱うことから，法改正を行なって協会の設立の手続き，業務及び役職員の「秘密の保持」に係る規定を置いている．

また後段の改正 NICT 法では，5 年間の時限措置として，パスワード設定に不備のある IoT 機器の調査（特定アクセス行為）を，NICT が行なうことができる旨の規定を新設している．この調査結果を協会経由で電気通信事業者に情報提供して，情報提供を受けた電気通信事業者は，パスワード設定に不備のある機器に係る利用者を特定して注意喚起を行なう仕組みになっている．NICT の行なう調査行為は，不正アクセス禁止法に該当する行為であるため，不正アクセス禁止法の特別法として NICT 法を改正したものである[61]．

このような規定が新設された現状を，前述の「情報共有の発展段階」と対比すれば，わが国もやっと第 4 段階から第 5 段階に移行しつつあるかに見える．しかし，そこで扱うことが可能な情報はシグナチャーなど形式化されたマルウェア情報にとどまり，attribution の解明に役立つログ情報は含まれていない．これでは，国内限りの情報共有は可能かもしれないが，国際的には不十分である．

なぜなら，情報の共有が可能な条件を一般化して言えば，① 当事者間に信頼関係があること，② 当事者が保有する情報の量と質において著しい差がないこと（ほぼ対等であること）の 2 条件が不可欠と思われるからである．この条件は，軍事情報の共有を定める GSOMIA（General Security Of Military Information Agreement）の前提をなすものであるが[62]，インテリジェンス情報など高度の機密性が求められる情報を共有する場合には，一般原則になり得るであろう．

5.4 情報保全のあり方

機微情報を共有する場合には，「情報保全」（Information Security = InfoSec）の手続きを定め，これを遵守する必要がある．本稿の文脈では「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」が「情報保全」の基本になる。情報の保全が不完全で，窃用や漏示が生ずれば，特定の個人に甚大な被害が及ぶほか[63]，国家の信頼が損なわれ長期間にわたって国際社会で不利益を被るかもしれない．前節における条件 ① の信頼関係が崩れれば，情報共有そのものが途絶

より行なわれるものをいい，電気通信事業者がその業務上記録している通信履歴の電磁的記録により，送信元の電気通信設備を合理的に特定できる場合に限る.」となっている（電気通信事業法 116 条の 2）.

61 他方，経済産業省は，サイバー対策が一企業内にとどまらず，グループ企業や部品・材料の供給先なども含めた「サプライ・チェーン全体」として確保されていなければならない時代になったとの認識の下で，企業間で営業秘密をシェアする場合に準じて，こうした情報も「限定提供データ」として不正競争禁止法で守る改正案を成立させた．グループ企業間で「脆弱性情報」を共有すれば，この規定で守られるのではないかという見方があるが，その細部は検討中のようである．

62 日韓両国の間の GSOMIA 継続の是非は，まさにこの 2 条件が満たされるか否かにかかっていると考えられる．

63 わが国の個人データ保護に関する議論は，ほとんど「消費者」である個人を念頭に置いたものだが，最も甚大な被害が生じたのは，イスラム教関係の情報提供者の名簿が流出した「警視庁国際テロ捜査情報流出事件」である．この事例では原告 14 名に対して合計 9020 万円の損害賠償が認められ，通常の個人データ流出事例とは桁違いであった（2010 年 10 月 29 日発覚，2016 年 5 月 31 日の最高裁判決で確定）.

える恐れもある.

この点に関する，わが国の理解は極めて遅れている．それは，わが国の企業風土が人的関係を重視し，手続きを通じてシステム化を進めることに気乗り薄なことと深く関係しており（林・淺井・田川 [2011]），その端的な例が「マニュアル」を評価しないことである[64]. 有体物が中心の時代, あるいは製造業が中心の時代にはそれで良かったかもしれないが，自律システムがインフラになった現代では，手続きを重視し「誰がやっても同じ結果が得られる」ように，システム化することが不可欠と思われる.

そこで準拠すべき規範は何かというと，やはり軍事情報やインテリジェンス情報を管理する基準に勝るものはないであろう．そこでは，a) 取り扱う情報に軽重を付ける（classification），b) 取り扱う人の資格を審査する（security clearance），c) この両者の組みあわせで Need-to-Know がない限り当該情報へのアクセスを許さない，d) 情報の窃用・漏示を厳しく罰する，の 4 つの手順が定められている.

ここで a) では，取り扱う情報を top secret，secret，confidential，unclassified に分けるのが一般的である．しかし米国では，unclassified の再分類が 100 種類近くになったので，新たに CUI（Controlled Unclassified Information）として再整理しつつある．b) は一種の資格審査であり，米国では資格取得者が再就職で有利になるなど，一種の合法的 discrimination ではないかとさえ言われている[65].

a) b) において参考になるのは，やはり米国の実例である．「ます隗より始めよ」で，連邦政府の情報管理体制を整備する法律（FISMA = Federal Information Security Management Act of 2002）を作り，CISO（Chief Information Security Officer）を必須ポストとするほか，自らに「情報行動規範」を課す．同時に，政府調達等を通じて民間にもそれに沿った運用を求める（Office of Management and Budget 所管）．そして，NIST（National Institute of Standards and Technology）が SP（Special Publication）シリーズによって，具体的な手続きをマニュアル化する，といった形で情報管理を手続面から枠にはめている.

c) は，これらの背後にある大原則ではあるが，これを強調しすぎると情報の共有が進まないため，Need-to-Share とのバランスが必要だとの議論を呼んでいる．そして最後に d) 守秘義務違反に対する罰則の強化である.

サイバーセキュリティ協議会参加者には, サイバーセキュリティ基本法 17 条 4 項違反の罪として, 1 年以下の懲役または 50 万円以下の罰金が科される（同法 38 条）が，これは一般公務員の守秘義務違反と同程度である（国家公務員法 100 条，109 条）．これを，民間企業の営業秘密の侵害罪や特定秘密漏示罪（いずれも刑の長期は 10 年以下の懲役）と同程度に引き上げることは，秘密の内容から見て当然ではないかと思われる[66].

上記の 4 原則は，特定秘密保護法の制定によって，わが国でもやっと法的に認め

---

[64] デジタルネイティブの若者の間では，西欧的なマニュアル文化に対する抵抗は少ないが，世代が上に進むに連れて，「経験と勘」に偏りがちである.

[65] ちなみに米国では，クリアランスを受けた人が 500 万人もいると言われている.

[66] 厳罰化は 5.2 節の第 4 段階以降の「公益利用のためのログのバルク知得」の場合だけでなく，第 3 段階までの「自己利用」の場合の「漏示・窃用」に関しても必要だと思われるが，そのためには「秘密保護法とは何か」という基本的検討が必要であろう．この点に関しては，林 [2017] 参照.

られるようになったが，まだまだ世間に知られていない．そこで，わが国の民間企業は, 準拠すべき手順として, ISO（International Organization for Standardization）が定めた ISMS（Information Security Management System[67]）や，米国 NIST が推奨する Security Framework[68] など国際的なものや，わが国の内閣サイバーセキュリティセンターが定めた「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）[69]」などを参考にし，あるいは準用しているのが現状である．

これは前述のように,「情報共有の発展段階」として，やっと第 4 段階から第 5 段階に移行しつつあるかに見えるレベルでは，やむを得ないこととも考えられるが，一日も早く「情報保全」の重要性に気づき，手続きを整備することが期待される．その意味では，前節で述べたとおり，認定送信型対電気通信サイバー攻撃対処協会における役職員の「秘密の保持」に係る規定が新設されたことは，地味だが重要な第一歩と評価できよう[70].

5.5 情報のライフ・サイクル全体の管理

ところで「情報保全」を検討する際の前提として明確にしておきたいのは，それが継続的な作業であって，一時点ですべてを決することはできないという事実である．これは個人データの扱いにも言えることで，世界の先頭を走っている感がある EU の GDPR（General Data Protection Regulation）における「処理」（Processing）の定義が，以下のように広範なものであることと通底するものである[71].

しかし，これは理念としては当たり前のようでいて，実行が難しい．特に機微なデータを知得する場合に,「データ主体の同意」をどうとるかを考えると，上記の各プロセス毎に同意をとるのはビジネス上煩瑣に過ぎる．そこで，最初のデータ取得時に「事後の扱いを含めた包括的同意」で十分だと考えたくなる．しかも，それが利用者の「使いやすさ」にもつながるケースがあるので,「利用者からも支持されている」と思いがちである．このような傾向は「取得時重視主義」を生むことにつながる．

そのような視点から見ると，本稿の主題であるログに関して，どのような知得が認められるかという議論よりも，どの程度の期間ログを保存しておくのが妥当か，という点に議論が集中していることが興味深い．

プライバシーに敏感な EU でも，一時は「通信が行なわれた日から最低 6 ヶ月，最大 2 年間データが保存されることの確保」し,「①固定通信及び移動通信については 18 ヶ月以内に，②インターネットを利用する通信については 36 ヶ月以内に，データを保全するための体制を構築しなければならない」と指令していたが[72]，2014

[67] https://isms.jp/isms/
[68] https://www.nist.gov/cyberframework
[69] https://www.nisc.go.jp/materials/index.html
[70] サイバーセキュリティ協議会に参加するメンバーにセキュリティ・クリアランスが行なわれない，などとは先進国からすれば驚きではないだろうか.
[71] GDPR 第 4 条（2）.「処理とは，自動的な手段であるか否かにかかわらず，個人データまたは個人データの集合に対して行なわれるあらゆる作業または一連の作業をいう．この作業は，取得，記録，編集，構造化，保存，修正または変更，復旧，参照，利用，移転による開示，周知またはその他周知を可能なものにすること，整列または結合，制限，消去または破壊することをいう.」
[72] Data Retention Directive (Directive 2006/24/EC)

年4月にこの規定がEU司法裁判所判決により無効とされた[73]，という歴史を持つ[74].

わが国の場合，ログの保存期間を法律で定めたものはなく，「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」[75]に拠っている．このガイドラインの10条1項では，「原則として利用目的に必要な範囲内で保存期間を定める」ことと，その後は遅滞なく消去することが規定されている．ただし「当該個人情報を消去しないことに特別な理由があるとき」はその例外とされており，「捜査機関から刑事事件の証拠となり得る特定の個人情報（通信の秘密に該当するものは除く）について保存しておくよう要請があった場合」が，例示されている(10条解説(5)).

そして保存期間については，「通信履歴のうち，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，（中略）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カ月程度の保存は認められ，（中略）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.」としている（同上解説）.

また，この論点は「通信の秘密」の保護対象が「電気通信事業者の取扱中に係る」ものであるとの要件と関係してくる．1963年の吉展ちゃん誘拐事件において「（犯罪捜査の過程で）捜査官憲が，受信者の同意を得て，通話の内容を録音することも『通信の秘密』に触れるものではない」という（電話中心時代の）解釈がなされているからである.

そこでは，「電気通信事業者の取扱中に係る通信」とは，「『発信者が通信を発した時点から受信者がその通信を受けるまでの間における通信』をいうのだから，既に受信され受信者の支配下にあるものは含まれない」とされており，有権解釈（電気通信法コンメンタール編集委員会 [1973]）も学説の大勢も，これを受け入れていた（前田 [1986] における片桐解説）.

しかし，この解釈をインターネットにそのまま適用するには，2つの障害がある．1つは，インターネット以前の通信形態である回線交換方式はstraight-forwardであるのに対して，インターネットのパケット交換はstore-and-forwardと対照的な点である．前者ではログが残らないのが常態であるのに，後者ではログを残すことが前提であり（林 [1984]），それだけ活用の魅力もあるが危険もあることになり，前者の時代の解釈をそのまま適用することに疑義がある.

第2の障害は，「他人が違法に録音した通信内容を，後刻入手し，第三者に聞かせた」行為も，「取扱中に係る通信の秘密」を侵したことになるという，今世紀に入ってからの最高裁の判決である[76]．この判決は直接，上記の法制局解釈を否定するものではないが，少なくとも「受信者に到達すれば受信者の支配下に入る」と直線的

[73] https://www.zdnet.com/article/eu-data-retention-directive-thrown-out-by-european-court-of-justice/
[74] ドイツ国内法についても，憲法裁判所による違憲判決が出ている．http://www.lait.jp/copyright/copyright_world570.html
[75] 平成29年総務省告示第297号 http://www.soumu.go.jp/main_content/000603940.pdf
[76] 最二小決2004年4月19日 刑集58巻4号281頁

に結びつけることに，疑問を呈したものと評価されるべきであろう[77] [78].

このように，ログなどの情報の知得だけでなく，知得した後の管理や保存期間等も含めて，情報の発生から死滅までの全体を管理することを，情報学では「情報のライフ・サイクル管理」と呼んでいる．サイバーセキュリティの観点からは，いつ何時窃取や漏洩が起きるかもしれないのだから，ライフ・サイクル全体を管理する必要性は，他の目的の場合よりも高い．この点も含めた，「情報保全」の仕組みを構築することが求められている．

その場合にも，ログの利用は一面でサイバーセキュリティの向上に資するものの，同時にプライバシー侵害の危険も内包していることを忘れてはならない．現在，大手プラットフォーマによるログを利用した行動ターゲティング広告が問題になっているが，サイバーセキュリティ対策としての利用も，一歩間違えば深刻な人権侵害に転じかねない．従って，「情報保全」の仕組みの中には，濫用防止の手順を組み込んでおかねばならないことは，言うまでもない

共著者は，サイバーセキュリティの研究に携わって 15 年近くになるが，セキュリティは写真でいう「ネガ」のようなものであり，その前提には「ポジ」として，「適切な情報管理」の手順が存在するはずだ，という感を強くしている[79]．情報管理が適切に行われているか否かは，学問で言えば「生理学」のようなものであり，セキュリティが破られた場合（セキュリティ・インシデント）を「病理学」的に追跡するだけでは，全体像を描くことができないのではないか，という感慨である．

6 暫定的なまとめと残された課題

本稿では，「通信の秘密」に関する「議論の空白」を埋めるために，以下の 6 点にわたるアンバンドルを試みた．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（通信履歴)」に触れる場合を切り分け，③ 違法・有害情報に対処する場合と，インターネット・サービスの安全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「ユーザの合意」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「バルクデータ」の扱いを別にする．

しかし，意気込みが強い割には，数多くの論点を消化しきれず，以下のような「つまみ食い」ができたに過ぎないことが悔やまれる．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を念頭に，ログの知得・利用を違法・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を探った．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

[77] 吉展ちゃん事件では，誘拐後の犯人からの電話を録音することの適法性が審査の対象であり，発信者の同意を求めることは論外であった．

[78] この判決によれば，インターネットを経由してコンピュータネットワークに蓄積されている情報に対する機密性侵害なども，「取扱中に係る通信の秘密」を侵害したことになるのだろうか？ もしなるとすれば，蓄積情報も「通信の秘密」の保護の対象になり，その影響は大きい．

[79] ネガとポジという比喩は，情報セキュリティ大学院大学の有田正剛教授に負う．

と目的内利用，そして早期の廃棄手続きをどのように担保するかである．

なお ⑥ においては，さし向き特定データを念頭に置き，バルクデータは今後の課題としたが，これはわが国のインシデント情報の共有が，現状では官民一体型の段階にあり，政府対応力を強化した官民一体型を将来の課題としていることに対応している．従って，残された部分はサイバーセキュリティにおける国家の役割に関する部分であり，民間企業に関する部分は本稿でほぼカバーできるのではないか，と思っている．国家戦略の役割に関しては，田川 [2013]，林 [2016]，情報セキュリティ大学院大学 [2017]，田川・林 [2017]，林・田川 [2018] 等において，予備的考察を行なっているので，参照いただければ幸いである．

[謝辞]

このような小論であっても，以下の引用文献に掲載させていただいた諸氏をはじめ，多くの方々の先行研究に助けられている．また今回は，個別にコメントをお願いした方々が，ご多用にもかかわらず適切な助言を下さったことに，特に感謝している．もちろん，本稿の記述内容に関しては，共著者が責任を負うべきことは当然である．

参考文献

[1] 生貝直人[2011]『情報社会と共同規制』勁草書房
[2] 石井夏生利 [2017]『新版 個人情報保護法の現在と未来』勁草書房
[3] 伊藤真・前田哲男 [2018]「サイトブロッキングと通信の自由」『コピライト』No. 600/ Vol. 58
[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] 海野敦史 [2018]「監視型情報収集と憲法 35 条 1 項との関係―『私的領域に侵入されることのない権利』を保障する意義」『情報通信政策研究』第 2 巻第 1 号
[6] 大石真・大沢秀介 [2012]『判例憲法（第 2 版）』有斐閣
[7] 金光昭・吉田修三 [1953]『公衆電気通信法解説』日信出版
[8] 阪本昌成 [1995]『憲法理論Ⅲ』成文堂
[9] 佐藤幸治 [2011]『日本国憲法』成文堂
[10] 佐藤慶浩 [2011]「証跡とログの区別～温故知新」デジタル・フォレンジック研究会第 182 号コラム　https://digitalforensic.jp/2011/11/10/column182/
[11] 宍戸常寿 [2016]「第 10 章 表現の自由」渡辺康行・宍戸常寿・松本和彦・工藤達郎『憲法 I　基本権』日本評論社
[12] 宍戸常寿 [2018]「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」2018 年 7 月 25 日,「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
[13] 渋谷秀樹 [2013]『憲法 第 2 版』有斐閣
[14] 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
[15] 鈴木秀美 [2008]「通信の秘密」大石眞・石川健治編『憲法の争点』Jurist 増刊
[16] 曽我部真裕[2013]「通信の秘密の憲法解釈論」『Nextcom』Vol.16, winter 号, KDDI 総研
[17] 多賀谷一照 [1995]『行政とマルチメディアの法理論』弘文堂
[18] 多賀谷一照・岡崎俊一・岡崎毅・豊嶋基暢・藤野克（編著）[2008]『電気通信事業法逐条解説』電気通信振興会

[19] 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, 情報セキュリティ大学院大学 http://www.iisec.ac.jp/proc/vol0005/tagawa13.pdf
[20] 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, 情報セキュリティ大学院大学 http://www.iisec.ac.jp/proc/vol0009/tagawa-hayashi17.pdf
[21] 電気通信関係法コンメンタール編集委員会 [1973]『電気通信関係法詳解(下)』一二三書房
[22] 永野秀雄 [2018]「米国の重要インフラに関するサイバーセキュリティと, セキュリティ・クリアランス法制(上)」『人間環境論集』 19 巻 1 号, 特に p. 42 以降
[23] 成原慧 [2012]「代理人を介した表現規制とその変容」『マス・コミュニケーション研究』 No. 80
[24] 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
[25] 成原慧 [2018b]「サイトブロッキングをめぐる法的問題」『法学教室』 453 号
[26] 長谷部恭男 [2012]「表現の自由と著作権」『コピライト』 8 月号
[27] 長谷部恭男 [2014]『憲法 第 6 版』 新世社
[28] 長谷部恭男ほか(編)[2013]『 ケースブック憲法 [第 4 版]』 弘文堂
[29] 林紘一郎 [2005]『情報メディア法』 東京大学出版会
[30] 林紘一郎 [2013]「通信の秘密:個人の権利か, 事業者の義務か」『警察学論集』66 巻 12 号
[31] 林紘一郎 [2014]「サイバーセキュリティと通信の秘密」土屋大洋(監修)『仮想戦争の終わり』 角川学芸出版
[32] 林紘一郎 [2016]「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』Vol. 34, No.3
[33] 林紘一郎 [2017]『情報法のリーガル・マインド』 勁草書房
[34] 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, 情報セキュリティ大学院大学 http://www.iisec.ac.jp/proc/vol0008/hayashi-tagawa16.pdf
[35] 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, 情報セキュリティ大学院大学 http://www.iisec.ac.jp/proc/vol0010/hayashi-tagawa18-2.pdf
[36] 林紘一郎・田川義博 [2019]「『通信の秘密』に関する3つのアンバンドリングの必要性」第 40 回情報通信学会大会報告 http://www.jsicr.jp/doc/taikai2019/spring/D-3.pdf
[37] 林紘一郎 ・ 淺井達雄・田川義博 [2011]『セキュリティ経営:ポスト 3.11 の復元力』勁草書房
[38] 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 (2019.6.15)
[39] 堀部政男 [2019b]「同(下)」NBL No.1149 (2019.7.1)
[40] 前田正道(編)[1986]『法制意見百選』 ぎょうせい, の「70 電話の逆探知, 通話の録音等」(片桐裕筆)
[41] Thompson II, Richard M. [2014] "The Fourth Amendment Third-Party Doctrine," Congressional Research Service https://fas.org/sgp/crs/misc/R43586.pdf
[42] Varian, Hal [2013] 'System Reliability and Free Riding,' in L. Jean Camp and Stephen Lewis (eds.) "Economics of Information Security," Kluwer Academic Publishing