サイバーセキュリティからみた「通信の秘密」

田川義博*

概 要

社会経済活動や国民生活は，インターネットに代表される情報通信ネットワークシステムに大きく依存して行われていて，その利用は大きな便益を生み出している．今後のSociety5.0 では更にその活用が進展すると見込まれている．一方，インターネット上では大量の違法有害情報が流通し，またサイバー攻撃の被害が拡大・深刻化している．加えてサイバーセキュリティが国家安全保障上でも新たな課題領域となっている．光と影の両面があるなかで，インターネットサービスを提供している電気通信事業者の役割が変質している．電気通信事業者は発信者から預かった通信をノータッチ（hands-off）で受信者へ届けることが本来的役割であり，「通信の秘密」の本来的意義である．ところがインターネットサービスでは，電気通信事業者が「通信の秘密」の制限を行う事例が多くなっている．

本稿は「通信の秘密」に関して，その役割の変質および「通信の秘密」の保護法益と制限の正当化根拠について，サイバーセキュリティに重点をおいて分析することを狙いとしている．1章で本稿のテーマ設定を行った後に，2章では「通信の秘密」の基本的枠組みを整理確認する．これを基礎として3章では電気通信事業者の「通信の秘密」に関する役割の変質を説明する．4章から8章が本稿の中心的内容である．まず4章では表現メディアとしてのインターネットへの関与、続いて5章では通信メディアとしてのインターネットへの関与について考察を行う．6章では「通信の秘密」の保護法益について考察を行い，7章では「通信の秘密」を制限する正当化根拠が，違法有害情報対策のための制限とサイバーセキュリティのための制限とでは，異なるとの説明を試みる．8章では，「通信の秘密」を制限する事例が増えているとしても，国際的視点から考えると「通信の秘密」の保護は依然として重要であることを指摘する．終わりの 9 章では，今後の通信技術の変化が電気通信事業法に及ぼす影響および Society5.0 における法の規律内容・手法の変化を探り，今後の「通信の秘密」の法的問題を検討するためのヒントとする．

1　はじめに

経済社会活動や国民生活が，インターネットに代表される情報通信ネットワークシステムに大きく依存して行われていて，その利用は大きな便益を生んでいる．今後のSociety5.0 では，サイバーとフィジカルが融合するような未来が語られていて，インターネットへの依存はより深まることが想定されている．

一方で，インターネット上では大量の情報が流通していると共に蓄積されていて，その

* 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

なかにある違法有害情報によって被害を受ける事例が多発し，誹謗中傷問題や偽情報(disinformation) に大きな注目が集まっている．

また，情報の中には個人情報，企業の機密情報および国家の機密情報が大量に蓄積されていて，サイバー攻撃によってこれらの情報の窃取やランサムウエアなどの被害が拡大・深刻化しており、IoT 機器の普及がこの傾向を加速している．この状況の中で，情報通信ネットワークシステム，およびその中を流通し，蓄積されている情報を守るサイバーセキュリティ対策が，より重要になっている．このサイバーセキュリティ問題は，国家安全保障や経済安全保障の文脈で語られることも多くなっている．

インターネットの光と影が混在するなかで，インターネットにおいては，電気通信事業者の役割が変質している．電気通信事業者の本来の役割は，預かった通信をノータッチ（hands-off）でそのまま運ぶことである．これが電話網時代から続く「通信の秘密」や「利用の公平」の規律である．

ところが，インターネットに関しては，預かった通信に関与を求められる又は認められる事例が多くなっている．電気通信事業者は「通信の秘密」の遵守を基本としつつも，どのような場合に例外的に「通信の秘密」を制限する行為を行えば良いかの判断に悩まされてきた．

「通信の秘密」の主管官庁である総務省は，「通信の秘密」の厳格な保護を旨として，個別事象毎に保護の例外を認めてきた．またこの保護の例外を認める場合には，各種の研究会・検討会において内容面および手続き面で慎重な検討を重ねている．電気通信関係団体は，その結論に基づいて自主的な規律として「ガイドライン」を策定して，そのガイドラインに従って業務運営を行っている．

また新たな事象が発生する都度，ガイドラインの新設・改正が繰り返され，場合によっては新たな立法や法律改正が行われている．

本稿では，2章において「通信の秘密」の基本的枠組みを整理確認したうえで，3章において電気通信事業者の「通信の秘密」に関する役割の変質を説明する．この2章・3章を基礎として，4章では表現メディアとしてのインターネットへの関与，ついで5章では通信メディアとしてのインターネットへの関与について考察する．

以上の2章から5章での考察を受けて，6章では憲法および法律レベルにおける「通信の秘密」の保護法益について考察する．次いで7章では例外的に「通信の秘密」を制限する事例に関して，「違法有害情報に関する関与」の場合と「インターネットサービスの安定的提供に関する関与」の場合では，制限する正当化根拠が異なるのではないかとの説明を試みる．

そして8章では「通信の秘密」の制限する事例が増えているとしても，「通信の秘密」の保護法益は普遍的であり，プライバシー，表現の自由，サイバーセキュリティに関する法制度とともに「通信の秘密」を保護することが，日本に対するEUの十分性認定の維持に役立ち，欧米との普遍的価値の共有にも資するものであることを指摘する．

終わりの9章では，今後の通信技術の変化が電気通信事業法へ及ぼす影響，およびSociety5.0 における法の規律内容と手法の変化を探り，今後の「通信の秘密」の法的問題を検討するためのヒントとする．

なお「通信の秘密」に関しては，研究者による多くの幅広く，緻密で的確な多くの著作があるが，本稿においては論旨を直截に進める意味合いから，その多くの論点を採りあ

げて論ずることができなかったが，本稿における考察には，林紘一郎氏を始め多く方々から示唆を得たことに謝意を表したい．また記述を簡素化する観点から，用語や具体的な事象の解説はあまり行っておらず，そのため論旨が把握しにくいことがあるかもしれないことを，予めお許しいただきたい．

2　「通信の秘密」の規定内容

2.1　憲法における「通信の秘密」

2.1.1　「通信の秘密」の保護内容と保護趣旨

憲法 21 条項後段で「通信の秘密は侵してはならない」との規定の保護内容について，佐藤[2011]は以下の 3 つを挙げている[1]．

① 公権力による積極的な知得行為の禁止
② 通信業務従事者による職務上知り得た通信に関する情報の漏えい禁止
③ 通信業務従事者による不当・差別的な取扱いの禁止

「通信の秘密」の保護法益について，鈴木[2008]は「表現の自由」と「プライバシー保護」の両方としつつも，プライバシー保護に重点を置く学説が多いとしている[2]．

また阪本[1995]は，「コミュニケーションの私秘性を確保することでプライバシー権を守るとともに，通信手段を用いた表現の自由をも保障する性格を有する」[3] と述べている．

歴史的にみると「通信の秘密」は，「信書の秘密」として近代憲法に登場した．通信は離れた場所にいる通信当事者間で行われるので，通信を運ぶことを第三者に依頼せざるを得ない．もしも通信を運ぶ第三者や公権力が通信の途中で通信内容などを見ることがあるとすれば，通信当事者は安心して通信することができない．鈴木の説く保護法益の基本にあるのは，この通信に対する通信当事者の期待であると考えられる．

2.1.2　「通信の秘密」の保護範囲と名宛人

「通信の秘密」の保護範囲については，例えば芦部[2011]は「通信内容はもとより，その差出人（発信人）または受取人（受信人）の氏名・居所および通信の日時や個数など，通信に関するすべての事項に及ぶ」としている．[4]

---

[1] 出典：佐藤幸治［2011］『日本国憲法』pp322～323 成文堂．なお，この③は電気通信事業法では，「利用の公平」（6 条）に対応していると考えられる．

[2] 出典：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 2008 年 12 月 15 日号 p136

[3] 出典：阪本昌成［1995］『憲法理論Ⅲ』p139 成文堂

[4] 出典：芦部信喜・高橋和之補訂［2011］『憲法 第 5 版』p214 岩波書店．憲法における「通信の秘密」には，「信書の自由」と「電気通信の秘密」の両方が含まれている．このため，差出人とか氏名・住所というような「電気通信の秘密」には含まれない事項もその対象とされている．電気通信においては，氏名・住所は契約者情報であって，「通信」によって得られる情報ではない．

このように「通信の秘密」の保護範囲については，通信内容だけではなく，電話の場合には発信番号，受信番号，発信日時，通話時間など，またインターネットの場合には発信者や受信者の IP アドレスや発信日時など，いわゆる通信の構成要素と呼ばれる事項も含まれるというのが通説になっている．

2.1.3 「通信の秘密」の名宛人と保護の限界

憲法における「通信の秘密」の規定の名宛人については，憲法が国家権力の行使に対する制限であるという立憲主義の立場からは，「通信の秘密」が国家権力の通信過程への介入を禁止する趣旨であることに異論はないと考えられる．

なお長谷部[2012]は，「憲法上の権利の多くがそうであるように，通信の秘密も絶対的に保障されるものではない．不可欠な公共の利益を実現するために適切に設定された必要最低限の制約は許される．」[5] と述べている．

公権力が「通信の秘密」を制限する法律としては，刑事訴訟法における郵便物等の押収（100条・222条），破産法における破産者宛ての郵便物や電報の破産管財人による開封（82条），関税法における郵便物の差押え（122条）などがある．[6] これらは電報の例を除き「信書の秘密」に関する例である．「電気通信の秘密」の例としては、1999年に制定された通信傍受法における通信傍受がある．

なお，一般の差押えの対象である「証拠物又は没収すべき物と思料するもの」（99 条）と比べて，刑事訴訟法100条では差押えが認められる要件が緩和されていることについては，「その合憲性には強い疑問がある」と，指摘されている．[7]

2.2 法律レベルにおける「通信の秘密」

2.2.1 「通信の秘密」を規定する法律

これには，電気通信事業法，有線電気通信法，電波法の 3 つの法律がある．

これらの法律に共通する点としては，「通信の秘密」の遵守をすべての人に科していること，および事業従事者の「通信の秘密」の侵害行為に対する刑罰が非従事者よりも重くなっていることがある．

またそれぞれの法律で条文の文言に差異があるが，総じて電気通信事業法がより厳格な遵守義務を科しているように考えられる．これは電気通信事業法が，「業として」の電気通信事業を対象としているためであると考えられる．以下，法律レベルの「通信の秘密」については，電気通信事業法の規定を基礎にして論を進めることとしたい．

---

[5] 長谷部恭男［2012］「第 4 章 通信制度」宇賀克也・長谷部恭男編『情報法』p68 有斐閣`

[6] 出典：前掲注5 p214

[7] 出典：前掲注2 pp322～323

2.2.2　電気通信事業法の「通信の秘密」に関する規定[8]（条文は巻末参照）

法3条において「電気通信事業者[9]の取扱中に係る通信」の検閲の禁止が規定されている．法4条 1 項では，「電気通信事業者の取扱中に係る通信の秘密」の侵害禁止が規定され，2 項では，電気通信事業の従事者の「電気通信事業者の取扱中に係る他人の秘密」を守ることが規定されている．法4条は，「通信の秘密」の遵守を規定している基本的条項である．

法164条1項3号では，「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（中略）を電気通信回線設備を設置することなく提供する電気通信事業（下線は筆者付加）」は，電気通信事業法上の届出・登録が不要とされている．

具体的な例としては，電子メールマガジンの配信，各種情報およびソフトウエアのオンライン提供，Web サイトのオンライン検索，オンラインストレージ，電子掲示板などがある．[10]

法164条 1 項の適用を受ける電気通信事業は，電気通信事業法の適用除外にはなるが，法3条（検閲の禁止）および法4条（通信の秘密）については適用されることが同条3項に規定されている．

法179条では法4条1項違反についての罰則が規定されていて， 2年以下の懲役又は100万円以下の罰金となっている．但し電気通信事業の従事者の違反については，懲役3年又は罰金200万円以下となっていて，刑罰が加重されている．

また電気通信事業の従事者に罰則が科された場合には，いわゆる両罰規定が法190条において規定されている．

なお法4条2項の「他人の秘密」に関する違反については，法179条の刑罰が適用されないというのが通説である．

法28条では，「通信の秘密」の漏えいなど重大事故の総務大臣への報告義務が規定され，また法29条1号において，「通信の秘密」の確保に支障があるときは，総務大臣は電気通信事業者に業務改善命令を出すことができると規定されている．

2.2.3　「通信の秘密」に関する判例

(1)NTT 東西が脅迫的電報の受付・配達を差し止めることを認めなかった判決

通信当事者から預かった通信をノータッチで運ぶことが電気通信事業者の本来的役割

---

8 電気通信事業法の条文を表記する場合には，以下「法 OO 条」と表記する．

9 法2条で用語の定義が与えられている．まず電気通信の定義（1号）から始まり，電気通信を行うための設備を「電気通信設備」（2 号），その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ことを「電気通信役務」（3 号），電気通信役務を他人の需要に応ずるために提供する事業を「電気通信事業」，そして最後に電気通信事業を営むことについて，法9条の登録及び法16条の届出をした者を「電気通信事業者」と定義している．（下線は筆者付加）

10 電気通信事業法上の登録・届出を要する事業，登録・届出を要しない電気通信事業（164条1項の適用事業）および非電気通信事業の区分に関しては，以下を参照．総務省「電気通信参入マニュアル[追補版]」令和元年 5 月 22 日　最終決定

であり，「通信の秘密」の遵守は電気通信事業者の重要な法的義務である．

この電気通信事業者の本来的役割を明確に示した判決として，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大阪地裁判決がある．

判決では，「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（下線筆者付加）」とされた．（大阪地判平成 16 年 7 月 7 日 判時 1882 号 87 頁）

上記判決では，NTT 東西が電報内容をチェックして，脅迫的な電報であると判断した場合に差し止めることが，預かった通信（この場合は電報）をノータッチで運ぶとの電気通信事業者の本来的役割違反であることを，「職務の性質からして許されない違法行為」との文言で述べたものである．

(2) 検証物提示命令に対する抗告棄却決定に対する許可抗告事件[11]

この事件で最高裁は，「電気通信事業法 4 条 1 項が通信の秘密を保護する趣旨は，通信が社会生活にとって必要不可欠な意思伝達手段であることから，通信の秘密を保護することによって，表現の自由の保障を実効的なものにするとともに，プライバシーを保護することにあるものと解される．電気通信の利用者は，電気通信事業においてこのような通信の秘密が保護されているという信頼の下に通信を行っており，この信頼は社会的に保護の必要が高いものということができる．」述べている．この指摘は，本稿で述べる論旨と一致する指摘であると考えられる．(最決令和 3 年 3 月 18 日判例集未搭載)

(3) 通信の秘密を侵したことを理由とする交換手の懲戒免職処分を有効と認めた判決

これはいわゆる「福知山電報電話局事件」として知られている事案である．電電公社の電話交換手Ａが，痴漢に襲われた旨の 110 番通話があったとの話を隣席の同僚Ｂから聞いて部外の知人に話をしたことから，関係者が迷惑を蒙ったことが新聞等に報道され，電話交換手 A が懲戒免職になった事案である．

本判決は，この懲戒免職処分について無効を求めた事案であるが，一審では原告が敗訴した．これに対して原告は控訴したが，高裁でも地裁判決が維持されたものである．

この事例は公衆電気通信法[12]違反としての刑事裁判ではなく，職員が「通信の秘密」を規定した公衆電気通信法に違反したことを理由に，電電公社が懲戒免職処分を行ったことに対する，労働裁判として行われたものである．（解雇無効確認等請求控訴事件，大阪高裁昭 41（ネ）665 号，昭 42・12・25 民 6 部判決，控訴棄却）

この事案がなぜ刑事裁判ではなく，労働裁判として行われたかの経過については不分明であるが，この事案は次(3)の事案とは異なり，電話交換手Ａの行為が公衆電気通信法違反に限定されている．当時の電話サービスでは電気通信事業の従事者以外の第三者

---

11 この最高裁決定は，成原慧氏に教えていただいたもので，ここに謝意を表したい．

12「通信の秘密」を規定していた当時の公衆電気通信法は，現在の電気通信事業法の前身の法律であるが，「通信の秘密」に関しては同一内容の規定が置かれていた．

が「通信の秘密」を侵害する可能性が低くかったことから，「通信の秘密」は，主として電電公社の社内規定によって維持されるべきもの，と理解されていたようにも考えられる．このため刑事事件として公衆電気通信法違反の立件とはしないで，電電公社の就業規則に基づく懲戒免職処分が行われ，これを不服とした被処分者が懲戒免職処分の無効判決を求め，労働裁判として扱われたのではないかと推測される．

(4) 1982 年のキャッシュカード偽造事件

本件は筆者が，電電公社北海道電気通信局秘書課長であった 1982 年 2 月に，発覚した事案である．本件は表彰・懲戒業務の担当として関わった事案であり，以下の記述は判決記録に基づく記述ではない．

本件はデータ通信業務の保守を担当する職員が，電話回線を介して伝送されていたデータ通信を知得（傍受）して，それによって得られた情報に基づき第三者名義のキャッシュカードを偽造し，その名義の銀行口座から預金を引き出した事案である．口座所有者が気づき警察に通報して捜査が始まり，当該職員が逮捕された．

その後当該職員が起訴され，札幌地裁で懲役 2 年 6 月の実刑判決になった．この事案では偽造カードを作成して，第三者の銀行口座から預金を引き出した犯罪行為の手段として，公衆電気通信法違反行為を行ったものであるが，当時の報道では「通信の秘密」の侵害行為として大きく報道された．

なお当該職員の行為は，公衆電気通信法の「通信の秘密」の侵害という重大な行為であることから，懲戒免職処分となっている．

(5) 検証令状による通信傍受が合憲とされた判例

この事案は通信傍受法の施行前に，検証許可令状により電話傍受を行うことの適否が争われた事案である．

最高裁は，通話当事者の同意を得ないで捜査機関が通信傍受を行うことについて，「重大な犯罪に係る被疑事件について，罪を犯したと疑うに足りる十分な理由があり，かつ，当該電話により被疑事実に関連する通話の行われる蓋然性があるとともに，他の方法によってはその罪に関する重要かつ必要な証拠を得ることが著しく困難であるなどの事情が存し，犯罪の捜査上真にやむを得ないと認められる場合に，対象の特定に資する適切な記載がある検証許可令状によって許される.」として，検証許可令状による電話傍受を認める判断を下している．[13]（覚せい剤取締法違反，詐欺，同未遂被告事件（平成 9 年（あ）636 号 同 11 年 12 月 16 日第三小法廷決定 棄却）

2.2.4 法 4 条の解釈問題

(1) 保護内容

保護内容としては，知得，窃用および漏えい（漏示）の 3 つであるとの理解が通説である．知得は「通信の秘密を知ろうとする意志をもって，積極的に知ること」，窃用は「本人の意思に反して自己または第三者の利益のために利用すること」，漏えいは「通信当事

[13] 判決内容の分析については，以下を参照．清水真［2017］「31 電話検証」『刑事訴訟法判例百選』pp70～71

者以外の第三者に，通信の秘密を漏らし，他人が知り得る状態におくこと」である．[14]

(2) 保護範囲

通説では，憲法と同じく通信内容と通信の構成要素の両方が保護範囲[15]とされている．通信の構成要素が保護対象に含まれる趣旨としては，通信の意味内容が推知され得るためとされている（下線は筆者付加）．

(3)「通信の秘密」と「他人の秘密」

法 4 条 1 項で「通信の秘密」が規定され，2 項で「他人の秘密」が規定されているが，憲法，有線電気事業法，電波法ではこの二つの区分は設けられていない．この区分については，以下のような三つの解釈があり得る．

第一は，「他人の秘密」の方が「通信の秘密」よりも保護範囲が広いとする解釈であり，この解釈が通説のようである．その例として，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が挙げられている[16]が，かなり限定的である．

またこれらは電報電話の事例であって，インターネットにおける事例は挙げられていない．インターネットにおいては，「通信の秘密」と「他人の秘密」の差分があまりないように考えられ，両者を区分して規定する意味がないように考えられる．このためこの解釈を採ることには疑問が残る．

但し，罰則の適用は法 4 条 1 項の「通信の秘密」の侵害行為のみで，2 項の「他人の秘密」への適用はないとされているので，両者の区分はその限りで有用である．[17]

第二は，法 4 条 1 項と 2 項は規律対象者と遵守義務が異なるとの解釈である．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，2 項は電気通信事業の従事者に対する規定であるとの解釈である．

すなわち，1 項の対象者については，知得，窃用，漏えいの全てが禁止されるのに対して，電気通信事業の従事者が，業務遂行上「通信の秘密」に該当する情報を知得するのは，正当業務行為であるため違法性が阻却される．従って，1 項と 2 項では規律対象者と遵守義務が異なることになる．

また 1 項では「通信の秘密は侵してはならない」と規定され，2 項では「他人の秘密」を守らなければならないと，文言上も使い分けられている．

---

14 出典：電気通信関係法コンメンタール編集委員会編［1973］『電気通信関係法詳解＜下巻＞』p40 一二三書房

15「通信の秘密」の範囲は，通話内容はもちろんであるが，通信の日時，場所，通信当事者の氏名，住所・居所，電話番号などの当事者の識別符号，通信回数等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すべてを含むものである．これらの通信の構成要素は，それによって通信の内容を探知される可能性があるし，また通信の存在の事実を通じて個人の私生活の秘密（プライバシー）が探知される可能性があるからである．出典：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』p38（財）電気通信振興会

16 この例については，以下の資料に記載があった例である．出典：「郵便・信書便における通信の秘密」、総務省郵便・信書便制度の見直しに関する研究会 2007 年 3 月 27 日資料 2

17「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罰則はなく，民事上・服務上の責任を問われるにとどまる．」と述べられている．出典：電気通信法制研究会［1987］『逐条解説 電気通信事業法』 p268 ぎょうせい

しかしこの解釈を採ると，2 項の従事者が「他人の秘密」を侵害しても，罰則はないということになって，事業従事者へ刑罰を加重している法 179 条と矛盾が生ずる.

そこで第三は，「他人の秘密」は，「通信の秘密」+ αであると解釈するが，「他人の秘密」の規定を設けたのは，従事者が知得することは通常は適法行為であるが，不正の知得，窃用および漏えいは，「通信の秘密」として刑罰の対象になるとの解釈である.[18]

この解釈と採れば，第一と第二の解釈の難を避けることができ，この解釈が妥当であるが，条文上この解釈を読み取るのはやや難しいように考えられる.[19]

(4) 2020 年改正電気通信事業法

インターネットサービスでは多層レイヤー化が進展していて，多くの事業者が連携して事業を行っている．国外企業であっても国内利用者に対して電気通信事業を行っている場合には，電気通信事業法の対象となると解されてきたが，「従来の運用のもとでは，国外に拠点を置き，国内に電気通信設備を有さずに電気通信役務を提供する者には，日本国内の利用者に向けて電気通信役務を提供する場合であっても，事業法の規律が及ばない状況になっていた.」[20]のが実情であった.

このため国内外事業者の競争条件を，equal footing にすべきとの指摘がなされてきた.[21] また適用がないことで，利用者保護が十分に図られないとの問題もあった.

この問題について 20 年改正電気通信事業法において，国外企業が登録・届出する際に国内代表者を指定する義務を科すとの規定が新設された（法 10 条 2 号及び法 16 条 2 号）．これにより報告義務（重大事故報告：法 28 条，報告及び検査：法 166 条）が生じ，ま

---

18 電気通信事業に従事する者は，職務上通信に関し他人の秘密を積極的に知得することが当然予想されるところ，単に業務上正当な行為として他人の秘密の知得行為は，2項及び1項違反とならず，その後これを第三者に漏えいし，又は窃用することが 2 項又は 1 項違反となることを明確にするためである．ただし，罰則は1項の通信の秘密を侵した場合に限られる．出典：前掲注16 p41

19 この第三の解釈によって、2．2．3における事例を考えてみたい．まず福知山電報電話局事件では，同僚Bの通話の監話（通話が正常に疎通されていることを確認する行為）は業務上正当行為であり，この監話内容が「他人の秘密」に該当する．この監話内容を同じ職場の A に話したことが「他人の秘密」の漏えいに該当するかについては両論があり得るが，A が職場外で監話内容を漏えいしたことは「他人の秘密」の侵害行為に該当する．

次にキャッシュカード偽造事件では，当該職員の職務内容が正確に分からないので，当該職員がデータ通信を知得（傍受）する行為が正当業務行為に該当するかについては判断できない．しかしいずれにしても，知得（傍受）した情報に基づいて偽造キャッシュカードを作成した行為は窃用に該当し，「他人の秘密」の侵害行為になる．

20 出典：山郷・小林・岡辺［2020］「令和 2 年改正電気通信事業法の実務対応～グローバル時代における OTT サービスを巡る実務的留意点」『NBL』No.1180 (2020.10.15)

21 2012 年にヤフーが無料 e メールサービス（インタレストマッチング)を始めるとの報道発表を行ったところ，総務省は法 4 条 1 項の「通信の秘密」の侵害に該当する可能性があるとの理由で難色を示した．しかし，Google が同様のサービスを始めたときには問題にならなかった．Google には電気通信事業法が適用されていないからというのがその理由である．同じサービスを提供しているのに，国内事業者は規制され，国外事業者は規制されないのは，競争条件を同じにして競争するとの equal footing に反するとの批判がなされた．この問題の 20 年改正電気通信事業法成立までの経過については，以下を参照．若江雅子[2021]『膨張 GAFA との闘い』中央公論新社．なお，本件は総務省が無料 e メールの導入を認めたことで決着した．

た業務改善命令（法 29 条）を出すことが可能になった.

さらに，国内事業者が法令違反行為を行った場合には罰則が科されるが，国外事業者の場合の法執行の困難性を考慮して，改正後の法 167 条の 2 において，法令等違反行為を行った者の氏名等を公表することができることになった.[22]

長年の懸案の解決に向けての着実な進展と評価できる.

(5)「事業者の取扱中に係る通信の秘密」の意義

「通信の秘密」の適用範囲としては，「電気通信事業者の取扱中の通信」と規定されている.[23]

なお，傍受を録音したカセットテープを借りて第三者に聞かせた場合も，「『取扱中に係る通信の秘密』を侵害したことになる」として被告人を罰金 30 万円に処した最高裁判決がある.[24]（最二小決平成 16 年 4 月 19 日 刑集 58 巻 4 号 281 頁）

また別の問題として，「取扱中に係る通信」であることから，携帯電話の基地局に係る位置情報のうち，個々の通信に利用される基地局情報は該当するが，通信を成立させるために登録する位置情報は「取扱中に係る通信」には該当しないので，対象外であると解されている.

さらに GPS 情報は，基地局の位置情報よりも精度が高く保護の必要性が高いものの，「取扱中に係る通信」に該当しないので，「通信の秘密」ではなく個人情報して保護される．このように GPS 情報の保護に関しては，情報の保護の強度が必要性の程度と異なっている.[25]

2.2.5 サイバーセキュリティと「通信の秘密」の対象範囲

被害が拡大・深刻化しているサイバー攻撃の動向については 5.2 において述べるが，本稿はサイバーセキュリティからみた「通信の秘密」の考察が中心的テーマであるので，サイバーセキュリティが対象とする範囲と「通信の秘密」が対象とする範囲がどう重なっているのか，または重なっていないのかについて把握しておくことにしたい.

---

22 20 年改正電気通信法の規定内容については以下を参照。立案担当者解説［2020］「電気通信事業法及び日本電信電話株式会社等に関する法律の一部を改正する法律」総務省『情報通信政策研究』4 巻 1 号

23「電気通信事業者の取扱中の通信」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時点までの間をいい，電気通信事業者（中略）の管理支配下にある状態のものをさす．（中略） 取扱中の通信とは，情報の伝達行為が終了した後も，その情報は保護の対象となるという趣旨である．従って，例えば通信終了後に電気通信事業者が保管している通信内容に関する記録（通信記録，交換証，頼信紙）も保護の対象になる.」出典：前掲注16 p35

24 この判決についての批判的な見解については，以下を参照．松原芳博［2012］「14 盗聴録音された通話内容の再生と電気通信事業法の秘密を侵す罪」高橋則夫・松原芳博編『判例特別刑法』pp123～125 日本評論社．松原は 4 条 1 項が「取扱中に係る」となっているのは、「現に取り扱っている」ないし「現に管理下にある」秘密に限定する趣旨であって，通信事業者の手を離れた秘密は 4 条 1 項の保護対象には含まれないと述べている.

25 総務省［2014a］「緊急時等における位置情報の取扱いに関する検討会 報告書 位置情報プライバシーレポート」pp6～8 2014 年 7 月

サイバーセキュリティ基本法 2 条において，サイバーセキュリティの定義[26]が示されている．そこではサイバーセキュリティの対象は，①「電磁的方式」による情報の漏えい，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，②情報ネットワークシステムの安全性および信頼性確保のために必要な措置が講じられ，その状態が適切に維持されていることをいうとなっている．すなわち，防御対象としては情報と情報通信ネットワークシステムの両方となっている．

一方、「通信の秘密」は，2.2.4 (5)で述べた「電気通信事業者の取扱中の通信」をその保護対象としている．従ってサイバーセキュリティでいう「情報」をその保護対象としているものの，情報システムに蓄積されている情報は保護対象となっていない．

また電気通信事業者が知得し，保管している情報は 2.2.4 (5)で述べたように，「通信の秘密」の保護対象となっている.さらに，情報通信ネットワークシステムは全体として，「通信の秘密」の保護対象外である．

このように「通信の秘密」の保護範囲は，サイバーセキュリティにおける防御範囲全体をカバーしているわけではない．

しかし，「通信の秘密」の保護対象外である情報システムおよび情報システムに蓄積されている情報へのサイバー攻撃は，いずれも「電気通信事業者の取扱中の通信」経由で攻撃が行われている．

また電気通信事業者が管理している電気通信ネットワークは，「通信の秘密」の保護対象外ではあるが，電気通信サービスを提供するためにその機能の維持が必要である．

従ってサイバーセキュリティの対象範囲であって，「通信の秘密」の保護範囲ではない電気通信事業者が管理する電気通信ネットワーク，クラウドを含む利用者の情報システムおよびそこに蓄積されている情報にも，「通信の秘密」の規定の効果が及んでいる．この意味合いでは，「通信の秘密」はサイバーセキュリティ全体に影響を与える規定といえる．

3　電気通信事業者の「通信の秘密」に関する役割の変質

3.1　ノータッチ（hands-off）から関与へ

2.2.3 (1)に述べた NTT 東西に脅迫的電報の受付・配達の差し止めを認めなかった判決では，「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伝送の媒体ないし手段として予定されている」と判示している．

本稿の用語で述べれば，電気通信事業者は預かった通信をノータッチ（hands-off）でそのまま運ぶことが，その本来的業務である．さもなければ、通信当事者は安心して通信することができない．これが「通信の秘密」を遵守する意味であり，電気通信事業者は長年この「通信の秘密」を重要な責務として遵守してきた．

この結果、「電気通信事業法において憲法と同じ通信の秘密が保護されており，しかも

[26] サイバーセキュリティの類似概念である情報セキュリティは，（情報と情報通信ネットワークシステムからなる）情報資産の機密性（confidentiality），完全性（integrity），可用性（availability）を守ることであるとの理解が一般的である。サイバーセキュリティ基本法 2 条の定義を情報セキュリティの定義を比較すると，ほぼ同一の
内容と対象になっているように考えられる．

それが非常に広くかつ強力は保護であると理解されている結果，一般的な個人情報保護・プライバシー保護を遥かにこえる義務が，電気通信事業者に課されている.」[27] という状態が長い間続いてきた.

「通信の秘密」がこのように理解されていたのは，個人情報保護法違反やプライバシー侵害の場合には，民事責任ないし行政責任を問われるのが一般的であるのに対して，「通信の秘密」の侵害に対しては，刑罰が科されることも一因かと考えられる.

しかしインターネット利用が普及・拡大してくるにつれて，この伝統に揺らぎがみられ，電気通信事業者が預かって運んでいる通信に介入することが，求められるまたは認められるようになってきた.

すなわち電気通信事業者が「通信の秘密」を保護するではなく，「通信の秘密」を制限するように役割が変質する事例が，いくつもみられるようになっている．なおこの役割の変質については，電気通信事業者の中でインターネット接続サービスを提供している ISP（Internet Service Provider）を中心に述べる.

この役割の変質には二つの理由があると考えられる.

第一に，インターネットにおいては，多くの人に見てもらうことを期待した情報発信（書込み）が増えていることがある．この場合には通信を利用するのは表現行為を行うためであって，秘匿性を有する利用とは全く異なる通信の利用形態となっている.

また多くの人がその情報（表現内容）にアクセスしている．このようにインターネットは，通信メディアであるだけではなく，表現メディアにもなっている.

インターネットでは，多くの人が名誉毀損，プライバシー侵害や著作権侵害情報のような権利侵害を含む「違法有害情報」にアクセスできるようになっているが，そのような表現内容によって被害を受ける人も出てくる.

本来であれば，権利を侵害されたとする人（被害者）が，表現内容を許容できないと考える場合には，表現行為者に是正措置を要求するか司法的な救済を求めることになる.

しかし通信を介した表現行為であり，また匿名表現も多いことから，発信者を特定できないことも多い．プロバイダ責任制限法では，特定電気通信役務提供者（定義は 2 条 3 号，ISP および違法有害情報にアクセスできるサービスを提供している事業者[28]）に対して，そ

---

[27] 出典：宍戸常寿［2013a］「通信の秘密について」『季刊 企業と法創造』35 号 pp20～21 2013 年 2 月

[28] 違法有害情報にアクセスできるサービスを提供している事業者が，電気通信事業法上の電気通信事業者なのか，164 条 1 項の電気通信事業を営んでいる事業者なのか，非電気通信事業者なのかが分かりにくい．例えば，プロバイダ責任制限法の「特定電気通信役務提供者」が，全て電気通信事業者または電気通信事業を営む者なのかには疑問が残る．前掲注11に記載した総務省「電気通信事業参入マニュアル（追補版）」がこの仕訳けをするための文書ではあるが，例えば SNS という文言はなく，どのカテゴリーに属するのかがすぐには分かりにくい．丸橋は「SNS を含むホスティングサービスプロバイダ」と述べて SNS をホスティングサービスプロバイダとして位置付けている．（出典：丸橋透［2021］「媒介者の責任」p19,『Jurist』February 2021, Number 1554）

また海野は，「電気通信事業法は，他人のサーバ等へのアクセス権限のみで電子掲示板を運営する個人等,『電気通信事業者にも電気通信事業を営む者にも該当しないが通信の秘密たる情報を直接取り扱う者』の取扱中に係る通信の秘密を保護していない.」と述べている．この原因として「近年になって急増したかかる者への立法的対応が追いついていない結果であり，今日的な『法律上の通信の秘密の間隙』となっているものと考えられる.」と指摘している．出典：海野淳史［2018］「法律上の通信の秘密の『間隙』とその立法的解決策」『情報通信学会誌』Vol.35 No.4 p85

の是正措置を採ることを求めることが認められている。

第二に，情報通信ネットワークシステムであるインターネットは，自律・協調・分散を旨として運営されているが，悪意の攻撃に対して脆弱性を有している．このためサイバー攻撃によって多くの被害が発生していて，電気通信事業者が提供しているインターネットサービスの安定的な提供に悪影響が生じている．

インターネットサービスを安定的に提供することは，電気通信事業者自身の責務であって，そのために「通信の秘密」の制限を認める法律やガイドラインが制定されている．すなわちこの場合の「通信の秘密」の制限は，電気通信事業者の業務上の必要性に基づく制限である．一方前述した第一の場合には，電気通信事業者に対して「媒介者の責任」を果たすために制限を求めるものであって，電気通信事業者が「通信の秘密」の制限を行うことでは同じであるが，その理由・動機は異なっている．

3.2 変質の背景：電話網からインターネットへ

「通信の秘密」に関する電気通信事業者の役割の変質は，電話網とインターネットの違いがその背景となっている．この違いには，ネットワーク技術・構成および機能・役割の二つがある．

3.2.1 ネットワーク技術とネットワーク構成の違い

(1) 電話網

電話網は競争導入後でも POI（Point of Interface）で相互接続されており，電気通信事業者が end to end で一元的に管理している．技術的な方式としては回線交換方式で，一旦発信者から受信者までの通信回路が設定されると，通信終了まで回路が保持されるので，guaranteed network と呼ばれている．

(2) インターネット

インターネットは network of networks であるが，このネットワークは「各ユーザが直接接続されている物理的なネットワークのことではなく，一つの AS 番号を割り振られているネットワークのこと」で，自律的なネットワークである AS が相互に接続されたネットワークである．

またインターネットでは「ネットワークとしての生存」が重視されていて，「さまざまなネットワークと接続できる」，「適切なコストで構築できる」，「新しいホストの追加が容易」という特徴があるので，何かあったときに代替機器を使えばネットワークを生存させやすくなる.[29]

電話網の場合には“intelligent network、stupid terminal”といわれていたように、ネットワークを一元的に管理する電気通信事業者が付与した機能が重要であった．一方インターネットでは，end to end の意味が逆転して，“stupid network、intelligent terminal”が

---

[29] 個々のネットワークは AS（Autonomous System：自律システム）と呼ばれる．この AS には世界で一意になるような番号が振られている．AS 番号を取得している組織の代表例は，OCN や Biglibe などの ISP であり，Google や Microsoft なども独自の AS 番号を取得している．

出典：あきみち・空閑洋平［2011］『インターネットのカタチ』pp26～28，pp14～15 オーム社

特徴である.

またインターネットにおける通信は，TCP/IP 方式によるパケット交換方式で行われていて，通信路を確保しない形で，細切れのパケットが送られるので，best effort 型と呼ばれている.

しかし guaranteed 型と比べて通信が届かないということでは必ずしもなく，東日本大震災の発生直後には，guaranteed 型通信が通信規制などで利用が大幅に制限されたのに対して，best effort 型のインターネットはかなりの程度利用できたことから分かるように，必ずしも劣った通信方式ではない。[30]

3.2.2 機能と利用の違い

(1) 電話網

会議電話のように 2 人を超える通話もあるが，通話は発信者と着信者間で秘匿性を有する形で行われるのが通常である．また通話内容は当事者が他の人に言わない限り，当事者間に留まる．また通話内容は，網内には蓄積されていない.

(2) インターネット

電子メールは 1 対 1 のメールと複数人への同報メールがある．また 3.1 で述べたように，SNS のように発信者は多くの人に読まれることを期待して，書込みをするために通信を利用している.[31] 従ってインターネットは，通信メディアであるとともに表現メディアでもある.

また電話網でも低速のコンピュータ通信は行われていたが，インターネットは主としてコンピュータネットワークとして利用されている．このため，stupid network，intelligent terminal として高度な機能を有するコンピュータが，端末として利用されている.[32]

このコンピュータネットワークでは，情報は伝送されるとともに蓄積されている．情報の中には，個人情報，企業の機密情報，国家の機密情報も大量に存在している．このためこれらの情報の窃取防止ために，サイバーセキュリティが重要な課題になっていることは，3.1 で述べた通りである。

以上の電話網とインターネットの違いが，「通信の秘密」に関する電気通信事業者の役割の変質の背景にあるといえる.[33]

---

30 東日本大震災発生時における電話網とインターネットの通信状況を見ても，best effort 型は必ずしも劣った通信方式ではない．但し，電話網でもインターネットでも，物理的な電気通信設備を利用して通信しているので，光ファイバーや通信ビルが損壊・流失した場合には，電話網もインターネットも利用できなくなる．このことについては以下を参照．田川義博［2011］「情報セキュリティからみた東日本大震災」『情報セキュリティ大学院大学紀要』Vol. 3

31 「通信」とは，「特定の差出人・発信人と特定の受取人・受信人との間で行われるコミュニケーション行為」をいう．出典：前掲注28 p15．通信をこのように解釈すれば，書き込みをするために通信する行為は，当然に通信ではないことになる.

32 電話網は，“intelligent network，stupid terminal”であったので，電話網に接続されている電話機などを「端末」と呼ぶことに違和感はなかった．しかしインターネットでは，“stupid network， intelligent terminal”となっているので，intelligence のある機器を「端末」と呼ぶのには違和感がある．15 年程前に「端末」との呼称に代えて何か良い名前を提案できないかと考えたが，良い名前が思い当たらず挫折した経験がある.

33 宍戸[2013b] は，「インターネットを規律する法的枠組みは，（中略） 二つの方向から重大な挑戦を受けている．（中略）

4　表現メディアとしてのインターネットへの関与

4 章ではまず表現メディアとしてのインターネットに関する分野において，電気通信事業者に対して「通信の秘密」を制限することを求める法律およびガイドラインについて，現状を確認する．次いでこの分野における最近の注目される政策・法制度動向として，海賊版対策として「通信の秘密」の制限であるブロッキング問題，違法有害情報への対応および 21 年改正プロバイダ責任制限法の成立経過と改正内容を採り上げる．加えて，侮辱罪の問題について述べる．

4.1　電気通信事業者に「通信の秘密」の制限を求める法律とガイドライン

5 章における通信メディアとしてのインターネットに関する分野では，電気通信事業者は自らの業務運営上の必要から，制限行為を行うことが「認められている」．これに対して表現メディアとしてのインターネットの分野では，制限行為を行うことは，電気通信事業者は自己の業務運営上の必要からではなく，情報の流通によって権利を侵害されたとする者（被害者）を救済するために，「媒介者の責任」を果たしている．この場合には電気通信事業者に対して制限行為を行うことが「求められる」ということになる．

表 1 電気通信事業者に対して「通信の秘密」の制限を求める法律及びガイドラン

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
根拠規定	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	違法有害情報の流通抑制	人命保護
制限の正当化根拠	正当行為 （刑法 35 条）	緊急避難 （刑法 37 条）

注：プロバイダ責任制限法 3 条に送信防止措置の規定があるが，この措置は表現内容に対するアクセス防止措置であって，「通信の秘密」を制限する行為ではない．一方，発信者情報は「電気通信事業者の取扱中の通信」の過程で知得されるものであって，「通信の秘密」の保護対象である．

4.2　インターネット上の海賊版対策におけるブロッキング問題

2018 年 4 月 13 日に知的財産戦略本部・犯罪対策閣僚会議が，「インターネット上の海

第一は（中略）国家がインターネット上の自由な活動を規制しようとするもの．（中略）第二は（中略）情報通信技術（ICT）の健全な発展にとって電気通信事業法制が桎梏となっている，との批判．」であり，第一の挑戦は公権力の関与の問題であり，第二の挑戦は「通信の秘密」を含む電気通信法制の見直し論であると指摘している．出典：宍戸常寿［2013b］「通信の秘密に関する覚書」長谷部恭男・安西文雄・宍戸常寿・林知更（編）『現代立憲主義の諸相（下）』pp490～491　有斐閣

賊版サイトに対する緊急対策案」を決定し公表した．この対策案では，「侵害コンテンツの削除要請すらできない海賊版サイト（例えば「漫画村」，中略）が出現し，著作権者等の権利が著しく損なわれる事態となっている.」として，「法制度整備が行われるまでの間の臨時的かつ緊急的な措置として，民間事業者による自主的な取組によって，「漫画村」（中略）などの 3 サイト及びこれと同一とみなされるサイトに限定して，ブロッキングを行うことが適当である.」と述べられている．

また「ブロッキングは他の方法による権利の保護が不可能であることなどの事情に照し緊急避難（刑法 37 条）の要件を満たす場合には，違法性が阻却される」としている．そして適切な管理体制の下ブロッキングの実施がなされるよう，（中略） 協議体を設置し，早急に必要とされる体制整備を行う」こととされた．

この動きが事前に報道されたことから，決定前から懸念の声があがるなか，知的財産戦略本部主催の「インターネット上の海賊版対策に関する検討会議」が設置された．この検討会議は，同年 6 月 20 日の第 1 回から 9 月 19 日の第 8 回まで開催された．途中で検討会議の他に勉強会が開催され，議論が重ねられてきた．

第 1 回の検討会議において，検討する論点として， ① 正規版流通の拡大によるコンテンツ視聴環境の整備，② 現行法令下での既存対策の検証及び実効性評価，③ 特に悪質な海賊版サイトに対する権利行使を可能にする法制度整備のあり方の 3 点が提示された．

この検討会議は政府の有識者の検討会としては，異例の経過を辿った．すなわち，第 8 回の会合で中間まとめを予定していたが，中間まとめができないほどに議論が対立・紛糾した．

議論が対立・紛糾したのは，海賊版対策として種々の対策を行うことが先決であるというグループと，既存対策には実効性がないのでブロッキングの法制化の検討を行うべきであるとのグループ間の対立が，主たる原因である．また事務局が，後者のグループ寄りとみられる資料づくりや運営を行ったことも，一因と考えられる．

前者のグループは，「通信の秘密」の保護法益と「著作権」の保護法益を比較衡量すると，「通信の秘密」の保護法益が優越するので，著作権侵害の新たな対策としてブロッキンを行うことには消極的なスタンスであったと考えられる．

またブロッキングは「通信の秘密」を侵害するものであって，「ブロッキングが絶対的に違憲ではないとしても、（中略）通信の秘密に対する重大な制約であり，その法制化の合憲性は慎重に判断するべき」[34] との立場をとっていて，第 1 回検討会議に提示された①と②の論点にウエイトを置くスタンスであったように考えられる．

これに対して後者のグループは，既存の対策を行っても実効性が低く，著作権等の被害は救済できないので，ブロッキングの法制化の検討を進めるべきとして，③の論点にウエイトを置いていたように考えられる．

事務局が第一回の検討会議で提示した前述の 3 つの論点を巡って，各回の検討会議では様々な議論が行われたものの，9 月 13 日の第 7 回検討会議で事務局が提出した「中間まとめ（案）」に対して，以下に代表される前者のグループの強い不信感が表明された．

---

[34] 出典：宍戸常寿［2018a］「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 回検討会議資料 4 p 8 2018 年 7 月 25 日

総合対策と銘打ちながら，ブロッキング以外の対策の実効性を高める方策を検討せず，仮に立法するとすればとしつつも法制度整備に関する実質が充填されないまま論点整理を行い，検討会議ではブロッキングについては両論併記の確認をする．そして検討会議以外の場でブロッキングの法制化を決定して，次期通常国会への法案提出を強行しようとするのではないか，との当初からの危惧が現実のものになりつつある．[35]

このように異例の経過を辿ったのは，検討会議を設置する契機になった 3 月 14 日の閣僚会議において，「ブロッキングの実施がなされるよう，知的財産戦略本部の下に（中略）協議体を設置」すると決定されたことが，基本的な原因であると考えられる．

この決定によって事務局である知的財産本部は，ブロッキングの法制化の課題を，既存対策の検証及び実効性評価よりも優先度の高い課題として，設定せざるを得ないことになったものと考えられる．

また同決定では，「法制度整備が行われるまでの間の臨時的かつ緊急的な措置として，（中略）緊急避難の要件を満たす場合には，（中略） 通信の秘密や表現の自由との関係でも，その侵害について違法性が阻却される」と述べられている．加えてブロッキングの実施は，（中略）あくまで民間事業者による自主的な取組として，（中略） 行うことが適当」と述べられている．

この決定では，特に悪質な海賊版サイトのブロッキングが，緊急避難の要件を満たすと判断しているわけではなく，民間事業者の自主的判断としてブロッキングを実施することが適当と述べているだけで，緊急避難の判断を民間事業者に委ねているようにも読める書きぶりとなっている．

「通信の秘密」の侵害行為は電気通信事業法で罰則が科されている行為であって，そのようなリスクを負ってブロッキングを行う判断をすることは，民間事業者としても苦渋の決断を迫られることである．自主的判断として NTT はブロッキングを準備が整い次第実施するとの方針を表明したが，実際には漫画村等の海賊版サイトが閉鎖されたために，実施には至らなかった．

この NTT の方針表明に対しては，NTT とインターネット接続契約をしている弁護士が，ブロッキングの差し止め請求を東京地裁に求めたが，2019 年 3 月 14 日付で敗訴判決があり，原告は控訴したが同年 10 月 30 日に東京高裁でも敗訴した．

また検討会議では，既存対策の実効性が低く，ブロッキングの法制化が必要であるとの主張が多くなされたが，「漫画村」サイトの元運営者が 2019 年 9 月に逮捕され[36]，2021 年 6 月に福岡地裁において著作権法違反と組織犯罪処罰法違反の罪で，懲役 3 年，罰金 1000 万円，追徴金 6257 万円の判決[37]が言い渡された．またこの判決に対しては，検察側，被告側双方が控訴せず，判決が確定している．[38]

なお，ブロッキングについては，現在は「ブロッキングに係る法制度整備については，

35 出典：宍戸常寿［2018b］「中間まとめ（案）に対する意見」第 7 回検討会議 資料 11 p3

36 出典：朝日新聞「漫画村運営者？逮捕 著作権法違反容疑」2019 年 9 月 24 日

37 出典：NHK「海賊版サイト「漫画村」元運営者に実刑」2021 年 6 月 2 日

38 出典：朝日新聞「漫画村、実刑判決が確定」2021 年 6 月 18 日

他の取組の効果や被害状況等を見ながら検討（内閣府及び関係省庁）」[39] とされていて，継続案件となっている．

4.3 違法有害情報への対応

違法有害情報については以下のように 4 つに分類[40]されている．

まず違法な情報[41]は、①「権利侵害情報」と②社会的法益侵害情報に分かれている．

①「権利侵害情報」では，名誉毀損，プライバシー侵害，著作権侵害および商標権侵害に関する情報が対象となっていて，「被害者」が存在する．これらの情報に対応するのが「プロバイダ責任制限法」および「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」を始めとするガイドライン[42]である．

② の「社会的法益侵害情報」は，必ずしも被害者が存在せず，社会的法益を侵害する 違法な情報であって，わいせつ罪に係る情報や覚せい剤取締法違反など薬物関連法に係る情報が該当する．

次に有害情報には，③違法行為の請負などの「公序良俗等に反する情報」がある．この公序良俗に反する情報は，「法令に直接違反するとは言えないまでも，受信者が誰であるかを問わず，流通されることが著しく不適切な情報である．（中略）一般的には，当該発信がなされるサービスの提供事業者が，利用規約においてこれらの情報発信を禁じ，利用規約等に則り削除等を行う形での対応がとられている．」[43] と説かれている．

また④発達段階にある「青少年に有害な情報」に関しては，「青少年インターネット環境整備法」が制定されていて，同法 21 条において青少年に有害な情報が発信された場合に，「特定サーバ管理者」に対して青少年閲覧防止措置を講ずる努力義務が科されている。

4.4 プロバイダ責任制限法の改正

4.4.1 プロバイダ責任制限法改正の経過

「2001 年に制定されたプロバイダ責任制限法は，（中略）インターネット上の情報流通により権利を侵害されたとする者（被害者）の救済と発信者の表現の自由等のバランスに配慮しながら，プロバイダ等の免責要件を明確にすることで削除等の送信防止措置を行

---

39 出典：内閣府等「インターネット上の海賊版に対する総合的な対策メニュー及び工程表について」p2 2021年4月9日

40 出典：総務省［2009］「インターネット上の違法・有害情報への対応に関する検討会～最終とりまとめ」p3

41 違法情報全体に関しては，事業者 4 団体によって「インターネット上の違法情報への対応に関するガイドライン」が制定されている．また事業者の自主的な取組を支援するために，「違法有害情報への対応等に関する契約約款モデル条項」も策定されている．このモデル条項では，利用者に対して禁止事項を列挙したうえで，情報等の削除等，児童ポルノ画像のブロッキングおよび青少年にとって有害な情報の取扱いなどについて， 標準的な規定を置いている．

42 個別分野毎に，「名誉毀損・プライバシー関係ガイドライン」，「著作権関係ガイドライン」，「商標権関係ガイドライン」がある．また（一社）セイファーインターネット協会（SIA）が，「権利侵害明白性ガイドライン」を作成している．

43 出典：上沼紫野［2021］「誹謗中傷と有害情報」『Jurist』February 2021, No.1554 p39

えるようにし(3 条)，さらに、発信者情報開示請求の仕組み(4 条)を設けたものである.」[44]

被害者の救済方法には，送信防止措置と発信者情報開示があるが，今回の改正は，「通信の秘密」の制限に係る発信者情報開示の規定内容を，大幅に見直そうとするものである.

検討の場として，総務省の「発信者情報開示の在り方に関する研究会」が設置された.同研究会での検討は 2020 年 4 月 30 日に始まったが，テレビ番組に出演したプロレスラーの女性が，SNS 上で激しい誹謗中傷を受けて 5 月 23 日に自死したことをきっかけにして，当初の検討課題よりもネット上の誹謗中傷にどう対処するかの問題が，集中的に議論されることになった.

同研究会では同年 8 月 31 日に「中間とりまとめ」を行い，12 月 22 日に「最終とりまとめ」を行った．この「とりまとめ」を踏まえて，2021 年 2 月にプロバイダ責任制限法の改正案が国会に提出され，同年 4 月 21 日に成立した．なお施行期日は，公布の日から起算して 1 年 6 月を超えない範囲内において，政令で定める日となっている．(付則 1 条)
また同研究会の中間とりまとめおよび総務省「プラットフォーム研究会」[45] の「インターネット上の誹謗中傷への対応の在り方に関する緊急提言」(2020 年 8 月)を受けて，総務省は同年 9 月に「インターネット上の誹謗中傷への対応に関する政策パッケージ」を公表した.

この政策パッケージにおいては，権利侵害情報(違法情報)と権利侵害に至らない誹謗中傷情報(有害情報)の切り分けを意識して，対策を実施するとしている．従って誹謗中傷への対策といっても，違法情報と有害情報の両方の対策が含まれていることに注意が必要である.

4.4.2 プロバイダ責任制限法の改正内容[46]

改正内容を大きく分けると，第一に，新たな裁判手続きの創設(発信者情報開示命令事件に関する裁判手続き)が挙げられる．従来の裁判手続きの他に，新たに非訟手続きが利用できることとなった.

現行法では，権利を侵害されたとする者(被害者)は，2 回の裁判手続きを経て発信者情報の開示を受けることになる．さらに損害賠償訴訟を提起するとすれば，合計 3 回の裁判手続きを経て初めて救済されることになる.

既存の手続きに加えて，改正後の新たな手続きでは，1 度の非訟手続きで発信者情報開示請求を行うことができるようになっている．これにより発信者情報の開示までの期間短

---

44 出典:宍戸常寿［2021］「インターネット上の誹謗中傷問題」『Jurist』February 2021 No.1554 p14

45 プラットフォーム研究会は，2021 年 9 月に誹謗中傷情報や偽情報を含む違法有害情報への対応，および利用者情報の適切な取扱いの確保を柱とする「中間とりまとめ」を公表している．この中間報告では，違法有害情報への対応と偽情報への対応を分けて記述している.

46 本 4.4.2 の記述内容は，以下の論文に基づいている．曽我部真裕「改正プロバイダ責任制限法の概要と成立の背景・経緯」『ビジネス法務』2021.8．また改正内容に関しては，「特集 インターネット上の誹謗中傷問題」『Jurist』February 2021 の 7 編の論文および「特集 3 改正プロバイダ責任制限法への実務対応」『ビジネス法務』2021 年 8 月の 5 編の論文を参照.

縮が可能になるとともに，「裁判所による柔軟な判断が可能」になる．この手続き改正と併せて，発信者を特定できなくなることを防ぐために，開示関係役務提供者（定義は改正法2条7号）が保有する発信者情報を消去してはならない旨を命ずることができる規定も新設された（改正法16条）．

第二に，開示する発信者情報の範囲についても拡大され，既に省令で開示が可能になった電話番号に加えて，ログイン時の情報が、改正法5条1項、3項により「特定発信者情報」として定義された．また通常の開示要件に加え，補充性要件が付加された（改正法5条1項3号）」．これに伴い，「プロバイダ責任制限法4条1項の発信者情報を定める省令」が，改正されている。

第三に，プロバイダ責任制限法の趣旨である，インターネット上の情報流通により権利を侵害されたとする者（被害者）の救済と発信者の表現の自由とのバランスをとるため，発信者の保護規定も加えられている（改正法6条 開示関係役務提供者の義務等及び12条 発信者情報開示命令事件の記録の閲覧等）．

4.4.3 法制審議会への侮辱罪改正の諮問

法務省は2021年9月16日に「侮辱の罪（刑法231条）の法定刑を1年以下の懲役若しくは禁錮若しくは30万円以下の罰金又は拘留若しくは科料とすること.」を法制審議会刑事法部会に諮問した．同部会は，同年10月6日に諮問内容通り総会に報告することを決定した.[47]

この諮問は4.4.1で述べたように，2020年5月23日にテレビ番組に出演したプロレスラーの女性が，SNS上で激しい誹謗中傷を受けて自死したことを契機としているとみられる．

このときSNSに書き込まれた誹謗中傷は300件ほどであったものの，書込み者の特定に時間がかかったこともあり，侮辱罪で起訴されたのは2件のみで，刑罰も科料9千円であったことについて，「法定刑が軽すぎる」との批判がでていた．「法務省は，厳罰化[48]や時効の延長で，ネット上の中傷を抑止し、摘発できる事件も増えるとみている.」[49]

5 通信メディアとしてのインターネットへの関与

5章ではまず，通信メディアとしてのインターネットに関する分野において，電気通信事業者に対して「通信の秘密」を制限することを認める法律およびガイドラインの現状を確

---

47 出典：法務省法制審議会刑事部会第一回および第二回会議資料．現行の侮辱罪の量刑は，拘留又は科料となっている．

48 島田は厳罰化を，処罰時期の早期化，犯罪行為主体の拡散，重罰化の三つと捉えている．出典：島田聡一郎［2007］「第1章 リスク社会と刑法」長谷部恭男責任編集『リスク学入門 3』p10，岩波書店．この捉え方によれば，今回の厳罰化は重罰化についての諮問である．

49 出典：読売新聞記事 2021年9月16日．なお，厳罰化しても必ずしも犯罪が減少するとは限らないので，更なる厳罰化を求める動きが出ることも想定される．犯罪と刑罰の基本的命題と現代的課題については，以下を参照．稲谷龍彦「刑事学の方法と課題」『法学セミナー』2019年4月号～2021年4月号

認する．次いで，2020年12月からの米国におけるサイバー攻撃例を分析する．さらに，日本のサイバーセキュリティ対処力の問題をとり上げる．そしてサイバーセキュリティに関する政策・法制度動向として，サイバーセキュリティ戦略本部の「サイバーセキュリティ戦略」，デジタル庁のサイバーセキュリティに関する役割，総務省サイバーセキュリティタスクフォースの「ICT サイバーセキュリティ総合対策 2021」および総務省の「電気通信ガバナンス検討会」の論議動向について述べる．そして最後に，国家安全保障の観点からサイバーセキュリティ問題について述べる．

5.1 電気通信事業者に「通信の秘密」の制限を認める法律およびガイドライン

表 2

事例	迷惑メール送信の防止	サイバー攻撃への対処	帯域制御
根拠規定	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	インターネットの安定的提供と受信者が希望しない電子メールの送信防止	インターネットサービスの安定的提供のためのサイバー攻撃に対する通信遮断等	インターネットの安定的提供のための特定アプリと特定ユーザに対する帯域制御
制限の正当化根拠	正当行為（刑法 35 条）	正当行為（刑法 35 条），正当防衛（刑法 36 条），緊急避難（刑法 37 条）	正当業務行為（刑法 35 条）

注：この迷惑メール送信の防止は、インターネットサービスの安定的提供に寄与するとともに，利用者を迷惑メールから守ることにも役立つ．

5.2 最近のサイバー攻撃の事例と特徴的事項

ここでは，2020 年 12 月からの米国における代表的なサイバー攻撃の事例をとり上げる．これらの事例は大きく分けると，第一の類型は，IT 企業のソフトウエアの脆弱性に対するサイバー攻撃を行い，そのソフトウエアを利用している政府機関や企業に不正侵入するという手口である．第二の類型は，ランサムウエア攻撃である．

第一の類型の事例としては，1）まず 2020 年 12 月に，ソフトウエア会社 SolarWinds の管理ソフトウエア Orion へのサイバー攻撃がある．このサイバー攻撃により NASA と連邦航空局を含め 9 つの政府機関が，サイバー攻撃を受けたことが確認された．このサイバー攻撃はロシアのハッカーによる攻撃であるとされている．

2）ついで 2021 年 3 月にマイクロソフトの企業向け電子メールソフト Exchange サーバの 4 つの脆弱性を狙った攻撃が行われ，Exchange サーバを利用している中小企業，地方自治体，学校など 3 万に及ぶ組織からメールボックスやアドレス帳が窃取された事例がある．

マイクロソフトはこの脆弱性を修正するパッチをリリースしたが，ハッカーたちが残したバ

ックドアを削除することはできなかった．このため FBI はこれまでにない裁判所命令を得て，バックドアが残ったままになっている数百台の Exchange サーバを実質的にハッキングしてバックドアコードを除去する対策を実施した．4 月には司法省はこの対策が成功したことを公表した．またネットワーク防御者が潜在的な侵入経路を特定できるよう，NSA は攻撃の詳細を公開した．

米国政府は、7 月に入ってから，このサイバー攻撃は中国国家安全保障省の仕業であると断定し，NATO，EU，英国，日本などの同盟国と共同で，中国の「悪質かかつ無責任なサイバー活動」を非難した．さらに司法省は，中国国家安全省に所属する 4 人のハッカーを新たに起訴すると発表した．

3）さらに 7 月に入ってから，IT 企業の Kaseya の法人向けソフトウエア（Kaseya VSA）が攻撃され，その利用企業でランサムウエア被害が拡大していることが顕在化した．被害者の多くが企業のシステム運用や保守を担当している MSP（Management Service Provider）であったため，攻撃やサーバの停止の影響が MSP の顧客にも及んだ．このため Kaseya と直接取引のないスウェーデンのスーパーマーケットのレジが動かなくなって，数百店舗が一時閉店を迫られる事態も発生している．このサイバー攻撃を行ったのは、ロシアのハッカー集団 Revil であるとの見方もある．

第二の類型は，サイバー攻撃によってシステムが停止し，そのシステムの復旧と引き換えに金銭を要求するランサムウエア型の攻撃である．この事例としては，1）米国の最大の産油地のテキサス州から東海岸のニューヨーク州へのパイプラインを運営する Colonial Pipeline への 2021 年 5 月に発生したサイバー攻撃がある．同社は操業を数日間停止したために，ガソリン不足が懸念される事態となった．同社はランサムウエア 440 万ドルをロシアが拠点とされる Darkside に支払ったが，司法省は支払われたランサムウエアのかなりの割合を回収したと発表した．

同社の CEO が連邦議会の公聴会に呼ばれ，長時間の質疑が行われたことでも分かるように，米国でのサイバー攻撃全般やランサムウエア型への対策に大きな関心が集まっている．

2）またブラジルの食肉大手 JBS がランサムウエア攻撃を受けて，北米とオーストラリアの食肉処理場のシステムが停止した．FBI は Kaseya と同様，ロシアのハッカー集団 Revil の仕業であると断定している．

これらのサイバー攻撃には，以下のような特徴があると考えられる．

1）IT 企業のソフトウエアの脆弱性へのサイバー攻撃によって，それらの IT 企業の多数のユーザに大きな被害がでた．しかし，ユーザが IT 企業経由のサイバー攻撃へ対処することは難しかった．
2）Colonial Pipeline が操業を止めたことで，リアル空間の経済活動にかなりの悪影響が発生した．また，ランサムウエアを支払った事例が多かったようである．
3）米国政府は，以下のサイバー攻撃対応を行って，大きな役割を果たした．
   ① バイデン大統領は、2021 年 5 月 12 日に Executive Order “Improving the Nation’s Cybersecurity” [50]を発出した．

[51] この Executive Order の内容については，以下を参照．永野秀雄［2021］「バイデン大統領による大統領令第 14028 号『国家のサイバーセキュリティの向上』について」『CICTEC Journal』2021.7 No.194

② 7 月にバイデン大統領は，ロシアのプーチン大統領と会談して，これらのサイバー攻撃に対して，ロシア政府のハッカー集団に対する支援を停止することを要求した．
③ 個々のサイバー攻撃における攻撃者の特定を行った．マイクロソフトの Exchange サーバの事例では，中国の国家安全保障省に所属する 4 人を起訴するなど，アトリビューション能力[51]が高いことが伺える．[52] また FBI のバックドアコードの除去やランサムウエアマネーの回収など，米国政府のサイバー攻撃対処力が高いことも実証されたように考えられる．
④ さらに，バイデン政権と連邦議会の双方で，サイバー攻撃対策の強化策についていくつかの提案が行われていて，現在検討が進められている．どのような結果になるかは現時点では予測できないが，サイバー攻撃による社会経済活動，政府機関の活動および国家安全保障分野での被害防止を図る観点から，強い問題意識に基づいて行動していると考えられる．

5.3 日本のサイバー攻撃対処力

英国のシンクタンクである IISS（The International Institute for Strategic Studies：国際戦略研究所）は，2021 年 6 月に“Cyber Capabilities and National Power：A Net Assessment”と題する報告書を公表した．この報告書は 15 か国のサイバー能力を 7 つの質的な指標によって，Tier1 から Tier3 に区分けしている．トップ能力の tier1 は米国，次の tier2 は中国など 7 か国，最後位の tier3 に入っているのは日本を含む 7 か国となっている．[53]

日本が最後位のグループに位置付けられた理由として，多くの企業がサイバー防御のコスト負担に消極的であること，および抑止的な（offensive）サイバー能力が憲法および政

なお，この大統領令と同時に出された Fact Sheet では，この Executive Order は SolarWinds，Microsoft Exchange Server，Colonial Pipeline へのサイバー攻撃に対応して発出したことが述べられている．

[52] 日本でも，2021年4月に警視庁が中国共産党の男を被疑者として，東京地方検察庁に書類送検した．この件について，2021年4月20日の内閣官房長官記者会見では，「本件捜査を通じて，契約された日本のレンタルサーバが，JAXA 等に対するサイバー攻撃に悪用されたこと，またその攻撃には中国人民解放軍61419部隊を背景に持つ『Tick』と呼ばれたサイバー攻撃集団が関与した可能性が高いことが判明したものと承知しております．」と述べている．出典：サイバーセキュリティ戦略本部［2021］「次期サイバーセキュリティ戦略」 p29．この被疑者を特定できたことは，日本で最初のアトリビューション成功例と評されている．2022 年度に警察庁にサイバー局新設構想があるので，今後サイバー攻撃に対する捜査力向上が期待される．

[53] もっとも，米国でもアトリビューションについては，困難ではあるが不可能ではないとされているようである．この困難さは，以下の記述に凝縮されていると考えらえる．“The painstaking work in many cases requires weeks and months of analyzing intelligence and forensics to assess culpability.”出典：“A Guide to Cyber Attribution” p2 Office of The Director of National Intelligence 14 September 2018

[53] IISS の報告書に関連して，サイバーセキュリティ戦略本部第 30 回会合（2021 年 7 月 7 日開催）でも，「我が国に関しては厳しい通信簿となったが，（中略）わが国の法制に関しては通信の秘密に関する憲法第 21 条がサイバー諜報能力にとってのバリアになっている，サイバー手段による反撃には自衛隊法の改正を要するとの記述があることに留意すべき．」との発言があった．またサイバー攻撃によって「被害を受けたときの対応の仕方，法整備などについて検討をお願い申し上げたい．」との発言もあった。出典：同会合議事概要 p5，p3

治的な制約があるために低位にあることがあげられている.

IISS 報告書では，他の組織が行っている評価方法は主にサイバーセキュリティに焦点を当てているが，IISS 報告書の方法はより幅広いとも述べている.[54]

また同報告書とも関連して，憲法 9 条の専守防衛と 21 条の通信の秘密の規定が,サイバーセキュリティ対処力向上の制約になっているとの論調が散見される.[55]

このようなサイバーセキュリティ対処力の現状に対して，次にサイバーセキュリティ対処力の向上策に関する政策・法制度の動向を分析する.

5.4 日本のサイバーセキュリティに関する政策・法制度の動向

5.4.1 サイバーセキュリティ戦略

サイバーセキュリティ戦略本部は，9月 27 日の第 31 回会合で「次期サイバーセキュリティ戦略」を決定した. また同日付で閣議決定されている.

この戦略においては，取組むべき 3 つのテーマ，そのテーマに関する課題認識と方向性および具体的施策が提示されている.

1) テーマ:経済社会の活力の向上及び持続的発展
課題認識:デジタルトランスフォーメーションとサイバーセキュリティの同時推進
具体的施策:サプライチェーン等の信頼性確保に向けた基盤づくり（Society5.0 に対応:サプライチェーン，データ流通、セキュリティ製品・サービス，先端技術）

2)テーマ:国民が安全で安心して暮らせるデジタル社会の実現
課題認識:公共空間化と相互関連・連鎖が進展するサイバー空間全体を俯瞰した安全・安心確保
具体的施策:クラウドサービスへの対応，サイバー犯罪への対応（警察におけるサイバー事案対処体制の強化など），包括的なサイバー防御の展開（ナショナル・サート機能の強化）及びサイバー空間の信頼性確保に向けた取組（経済安保の視点を踏まえた IT システム・サービスの信頼性確保:政府調達、重要インフラ、国際海底ケーブル等）

3)テーマ:国際社会の平和・安定及び我が国の安全保障への寄与
課題認識:安全保障の観点からの取組強化策として，「サイバー空間は国家間の競争の場となっている. 中国・ロシア・北朝鮮はサイバー能力の構築・増強を行い，情報窃取等を意図したサイバー攻撃を行っているとみられている.」「サイバー空間の安全・安定の確保のため，外交・安全保障上のサイバー分野の優先度をこれまで以上に高める（後略）」
具体的な施策:自由・公正かつ安全なサイバー空間の確保、防御力・抑止力・状況把

---

[54] IISS の報告書が言及した他の報告書とは，“the International Telecommunication Union’s Cybersecurity Index”，“the Potomac Institute’s Cyber Readiness Index2.0”，“the Harvard Kennedy School’s National Cybersecurity Power Index 2020” である. 評価指標はそれぞれの報告書によって異なっていることと，定性的な指標と定量的な指標の両方があるので，その相互比較を行うことには注意が必要であることについては以下を参照. 一田和樹「国家別サイバーパワーランキングの正しい見方」『ニューズウイーク日本版』 2021 年 7 月 15 日

[55] 例えば、「サイバー防衛，仮想空間の『グレーゾーン』憲法も壁に」 日経新聞，2021 年 7 月 21 日

握力[56]の強化など

今回のサイバーセキュリティ戦略は、①デジタル庁が発足したことを契機として，DX との同時推進を明示したこと，②サイバー攻撃に対する防御力，抑止力およびサイバー空間の状況把握力の強化を具体的施策で挙げたこと，③サイバー空間の公共空間化などサイバー空間が社会経済活動，国民生活，国家安全保障および経済安全保障のそれぞれとつながりが強まっていることを基本認識としていることが，特徴であるように考えられる．

これらの特徴的事項は，「サイバーセキュリティ戦略策定に際しての国家安全保障会議意見」にも述べられていて，デジタル庁と安全保障会議との連携を重視し，サイバー空間に関する政策の総合性ないし相互連携性をより強く意識した戦略となっているように考えられる．

5.4.2 デジタル庁のサイバーセキュリティに関する役割

2021 年 5 月12日に，デジタル社会形成基本法，デジタル庁設置法およびデジタル社会の形成を図るための関係法律整備法などが成立した．

デジタル社会形成基本法第6章においては，重点計画を策定することが定められている．世界最高水準の高度情報通信ネットワークの形成やサイバーセキュリティの確保等についても重点計画の対象になっている．サイバーセキュリティの確保等については，サイバーセキュリティ戦略本部の意見を聴いて、重点計画を定めることが規定されている．

またデジタル庁設置法においても，デジタル庁が上記重点計画を作成・推進することが規定されている(4 条 2 項 1 号)．

しかし，デジタル庁が作成・推進することになっている重点計画は，デジタル庁発足前の 2021 年 6 月 15 日に既に決定されている．この重点計画では，「デジタル庁は内閣サイバーセキュリティセンター（NISC） とも連携して，情報システム整備方針においてサイバーセキュリティについての基本方針を示す」こと，および NISC は「国の行政機関等のシステムに対するセキュリティ監査を行うことで，政府全体のシステムのセキュリティ確保を進める.」の 2 点が示されている.[57]

サイバーセキュリティの権限関係については，デジタル庁設置法 4 条 1 項 2 号(所掌事務)において，サイバーセキュリティ基本法 26 条(所掌事務等)1 号との関係について調整が図られている．また同法 8 条(デジタル大臣)5 号によって，関係行政機関の長への勧告権が認められている．

---

56 サイバーセキュリティ技術は，民生用にも軍事用にも両方に利用可能な「両用技術」であり，「明らかに民生利用しかできない技術を別にすれば，その研究技術情報の管理方法は，軍事研究や防衛装備品の調達に準じたレベルを維持することが求められる.」との指摘があるので，防御力・抑止力・状況把握力に関する技術は，民間企業などが利用する技術でも安全保障用にも転用されることがあると考えられる．

出典：林紘一郎［2021］「研究技術情報のセキュリティ管理」『情報セキュリティ総合科学』Vol. 13

57 高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議［2021］「デジタル社会の実現に向けた重点計画」pp57-58 2021 年 6 月 16 日

デジタル庁が作成・推進する重点計画は，デジタル社会形成法における基本理念および施策策定に関する基本方針に基づいて作成・推進される．この重点計画に基づいて，サイバーセキュリティ戦略本部が実際の施策を推進するとの法的な枠組みになっている．また NISC が担当するセキュリティ監査などによって，サイバーセキュリティ対策がより強力に進展することが期待される．

このようにデジタル庁の発足に伴って，次期サイバーセキュリティ戦略の一つ目のテーマである「DX とサイバーセキュリティの同時推進」が図られることになる．

5.4.3 総務省「ICT サイバーセキュリティ総合対策 2021」

「ICT サイバーセキュリティ総合対策 2021」（以下、総合対策 2021）は，2017 年 1 月から活動している「サイバーセキュリティタスクフォース」が策定したものである．このタスクフォースは，2017 年 10 月に「IoT セキュリティ総合対策」，2019 年 8 月および 2020 年 7 月に「IoT・5G セキュリティ総合戦略」を策定している．

今回の「総合対策 2021」は，2020 年 12 月に閣議決定された「デジタル社会の実現に向けた改革の基本方針」の下で進められていて，デジタル庁の新設，DX の推進，次期サイバーセキュリティ戦略との整合性をとる形で策定されたと考えられる．

また，「総合対策 2021」1 章では，閣議決定された上記基本方針やサイバーセキュリティ戦略に関して，かなりのページを割いて述べている．ついで 2 章および 3 章においては，総務省所管の具体的課題・施策の検討が行われている．

その内容としては，「サイバーセキュリティ戦略」と同じく，IoT のサプライチェーン対策，クラウドサービス，スマートシティなどの事項が取り上げられている．

以下では本報告書のなかで、「通信の秘密」に関する事項について分析する．

1）IoT 機器の運用段階での対策：端末側の対策としての Notice

「サイバー攻撃関連通信の約半数が IoT 機器を狙ったものである」ことが明らかにされた．この IoT 機器の脆弱性対策として，18 年改正電気通信事業法および改正国立研究開発法人情報通信研究機構（NICT）法（以下 NICT 法）が成立している．改正電気通信事業法では，第 2 章 電気通信事業に「第 8 節 認定送信型対電気通信設備サイバー攻撃対処協会（116 条の 2～116 条の 8）」の規定が新設された．この8章には，「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を漏らしてはならない（168 条の 4）」との規定がある．

また NICT 法では，NICT の業務として「特定アクセス行為」（定義は付則 8 条 4 項 1 号）を行うことが時限立法（平成 36 年 3 月 31 日まで：付則 8 条 2 項）として新設された．この規定に基づいて，サイバー攻撃に悪用されるおそれのある機器を調査し，電気通信事業者を通じて利用者への注意喚起を行う Notice が行われている．しかしこの実施状況評価では，対策の有効性には問題があることが述べられている（pp22～23）．

この現状分析を踏まえて，「現状の端末機器側での対応だけでは，端末の踏み台への悪用に適切に対応することが難しくなっていくことが予想される．（p11）」と述べられている．

2）今後は端末側の対策に加えてネットワーク側の対策が必要

この認識に基づいて，「サイバー攻撃に対する電気通信事業者の積極的な対策

(p13)」として，IoT セキュリティ対策の実効性を高めるために，「トラフィックが通過するネットワーク側でより機動的な対処」が必要であるとして，「インターネット上で ISP が管理する情報通信ネットワークでの対策」として，「電気通信事業者が自らトラフィックの流れ(フロー情報)を把握・分析して攻撃元の C&C サーバを検知」し，「この情報を電気通信事業者と共有し」，サイバー攻撃の予知を早期に捉えて対処できるようにするため，「通信の秘密の保護を図りつつ」検討を行うこと適当である[58]と述べられている.

3) IoT(機器)に関する研究開発計画の推進

SIP(戦略的イノベーション創造プログラム)の第 2 期(2018 年度～2022 年度)の計画の一つとして，「IoT 社会に対応したサイバー・フィジカル・セキュリティ研究開発計画」が進行中である.

この研究開発計画では，「サイバー攻撃の進化は留まることがなく，Society5.0 の社会ではその脅威はサイバー空間のみならず，フィジカル空間に対しても深刻な影響を及ぼしうる」との基本認識のもと，「IoT 機器やサプライチェーンの各要素について，セキュリティ確保(信頼の創出)とその確認(信頼の証明)を繰り返し行い，信頼のチェーン(連鎖)を構築することで，IoT システム・サービス及びサプライチェーン全体のセキュリティを実現」することを研究課題としている.[59]

5.4.4 総務省「電気通信事業ガバナンス検討会」

この検討会は，2021 年 5 月にスタートして，9 月 15 日に第 8 回検討会が開催されている. 検討会では，「通信サービスの提供環境が変化するなかで，通信サービスにおけるネットワークの仮想化などの技術進歩，クラウド活用や関与ステークホルダーの増加・複雑化等のサービス構造の変化，サイバー攻撃の複雑化・巧妙化およびサプライチェーンリスクなど経済活動のグローバル化の進展に伴い，情報漏えい，情報の不適正な取扱いおよび通信サービス停止のリスクが高くなることによって，個人的・社会的・国家的法益が侵害されるおそれが高くなっている」との指摘を行っている.

本検討会では，この状況認識に基づき「電気通信事業ガバナンス」の在り方を検討することを課題としている. ガバナンス確保のための具体的対策として，設備を対象とした対策に加えて，新たに情報に関する対策が必要であるとしている. この情報の中に，「通信の秘密」や利用者に関する情報が含まれている.

また第 5 回検討会では，事故報告・検証制度等の在り方についての報告[60]があった.この報告には，自然災害・サイバー攻撃を原因とする通信事故の報告制度の在り方が含まれている. この問題は，法 28 条の重大事故報告と法 166 条の報告及び検査に関係している.

---

58 フロー情報を把握・分析して，C&C サーバを検知する件については，「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 4 次とりまとめ(案)」が，2021年10月5日に公表され，意見募集中である.

59 出典:「戦略的イノベーション創造プログラム(SIP) IoT 社会に対応したサイバー・フィジカル・セキュリティ 研究開発計画」p1、p5、2021 年 7 月 19 日 内閣府科学技術・イノベーション推進事務局

60 この報告は，情報通信審議会 情報通信技術分科会 IP ネットワーク設備委員会 事故報告・検証制度タスクフォースによって行われた.

5.5 国家安全保障におけるサイバーセキュリティ

5.4.1で述べたように，「次期サイバーセキュリティ戦略」の三つ目のテーマである「安全保障への寄与」について，安全保障の観点からサイバーセキュリティがどう位置付けられているかとの視点から、節を改めてとりあげる.

まず「次期サイバーセキュリティ戦略」では，具体的な施策として「政府機関，重要インフラ事業者，先端技術を有する企業・学術機関等への攻撃や，民主主義の根幹を揺るがしかねない事例[61]も発生している.」との認識の下で，「国家を防御する力（防御力）サイバー攻撃を抑止する力（抑止力），サイバー空間の状況を把握する力（状況把握力）を高めつつ，政府全体としてシームレスな対応を抜本的に強化することが重要である.」と述べている.

対応主体としては，安全保障については内閣官房国家安全保障局が全体的とりまとめを行い，防御は内閣サイバーセキュリティセンターが中心となって担う，抑止は対応措置を行う省庁，状況把握[62]は情報収集・調査を担う機関が平素から緊密に連絡して進めるとの方針が示されている.

一方，安全保障分野におけるサイバーセキュリティについては，2018 年 12 月に閣議決定された「平成 31 年度以降における防衛計画の大綱について」および「中期防衛力整備計画（平成 31 年度～平成 35 年度）について」において述べられている．防衛計画大綱などには，サイバー空間を新たな防衛領域と位置づけて強化すること，および陸海空と連携して領域横断作戦も強化することが謳われている.

また，「サイバー領域における能力」として，「自衛隊の指揮通信システムやネットワーク」の防御力を引き続き強化するとともに，「有事において他国がサイバー攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力などの抜本的強化を図る.」[63] ことが強調されている．この「相手方によるサイバー空間の利用を妨げる能力」という文言は，「次期サイバーセキュリティ戦略」においても用いられていて，サイバーセキュリティ戦略と防衛大綱が整合性のある形で策定されていることを示唆しているように考えられる.

さらに，「独立と生存及び繁栄を経済面から確保する」観点から，経済安全保障体制の抜本的強化を図るべく，①サイバー攻撃等による技術流出防止体制の拡充，②国内においてサイバーセキュリティ製品・サービス・人材が安定的に供給される状況を作る，③NISC が主導するサイバーセキュリティに関する情報共有の徹底などが提言されている.[64]

---

61 米国の大統領選挙での他国からの意図的な偽情報（disinformation）の送信などを指しているものと考えられる.

62 この状況把握を行う機関の中には，インテリジェンス機関も含まれていると考えられる．本稿ではインテリジェンスについては言及していないが，「通信の秘密」に関係する重要な問題である.

63 出典：「平成 31 年度以降における防衛計画の大綱について」p18

64 出典：「新国際秩序創造戦略本部中間とりまとめ」pp14～15, pp24～25，自民党政務調査会，2021 年 5 月 27 日．なお，NICT のサイバーセキュリティ統合知的・人材育成システム（CYNEX）やセキュリティクリアランスについても言及されている．p14, pp20～21

6　「通信の秘密」の保護法益

2 章において「通信の秘密」の規定内容について述べたが，本 6 章では 2 章の規定内容の基本にある「通信の秘密」の保護法益の問題について考察する.

6.1　憲法における「通信の秘密」の保護法益

2．1．1で述べたように，憲法における保護法益としては，鈴木[2008]は「表現の自由」と「プライバシー保護」の両方としつつも，プライバシー保護に重点を置く学説が多いとしている.[65]

宍戸[2016]は，「プライバシー権の観念が発展した現在では，通信の秘密はその一局面を取り上げて明文で保障した規定」と述べるとともに，「通信の秘密は匿名による表現ないし親密者間の 1 対 1 の表現の自由を保障する意義を有する.」[66] とも述べている.

曽我部[2013]は，保護法益は「主として通信におけるプライバシーである」と述べるとともに，「通信事業が国営の時代にあっては，憲法の基本権としての通信の自由を観念する余地は乏しかった可能性がある」としつつも，「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」，その根拠条文を「13 条とするか，あるいはその関係の密接さを強調して，通信の秘密条項に改めて位置づけるということも考えられる.」[67] と述べている.

6.2　電気通信事業法における「通信の秘密」の保護法益

6.1 でみた憲法の「通信の秘密」の保護法益に対して，電気通信事業法に代表される法律レベルの保護法益は何であろうか？

石井[2013]は，「個人のプライバシーだけを保護法益として説明することは困難である。」としている．また，「通信の秘密の保護は，コミュニケーション内容が当事者の知らないところで知得されないという通信当事者の期待がその中核を形成している」と解すれば，「通信当事者が個人だけではなく，企業等の法人または団体を主体することも説明」でき，さらに「通信当事者の期待を保護するために，電気通信業務の適正かつ合理的な運用およびこれに対する社会的信頼をも，通信の秘密侵害罪が保護していると解すべきである.」[68] と述べている.

また，「通信の秘密の保護には，通信事業を利用する公衆の自由（通信の自由）及び社会インフラとしての通信システムの確保の要請が前提とされると解される」[69] との指摘もある．この「通信システムの確保」が「通信の秘密」の保護法益に含まれているとの解釈なのかは明確ではないが，「通信システムの確保」という社会的役割を法律レベルの

---

65 出典：前掲注 3　p136

66 出典：宍戸常寿［2016］「10 章　表現の自由」渡辺康行・宍戸常寿・松本和彦・工藤達郎著『憲法 I 基本権』p236　日本評論社

67 出典：曽我部真裕［2013］「通信の秘密の憲法解釈論」『Nextcom』2013 Winter Vol.16 pp19～20

68 石井徹哉［2013］「通信の秘密侵害罪に関する管見」千葉大学法学論集 27 巻 4 号 p123～124

69 出典：宍戸常寿「円滑なインターネット利用環境の確保に関する検討会（第 1 回）」p1　2017年10月26日

保護法益と考えるならば，「電気通信業務の適正かつ合理的な運用およびこれに対する社会的信頼」を保護法益とする前述の石井説と共通する解釈であると考えられる。

またこの「通信システムの確保」は，本稿の用語である「インターネットサービスの安定的提供」と同義であると考えられる.

「通信の秘密」の保護法益が，プライバシーなどの個人的法益を超えて，「電気通信業務の適正かつ合理的な運用およびこれに対する社会的信頼」との社会的法益までに広げる解釈について，2 点指摘したい.

1)「通信の秘密」の保護内容が，2．2．4で述べたように，知得，窃用および漏えいを禁止することであることは共通的理解であるが，この保護内容が「業務の適正・合理的運用およびそれに対する社会的信頼」が保護法益であるとの解釈にどう論理的につながるのであろうか？

2) 電気通信事業法 179 条に罰則が規定されているが，プライバシーなどが保護法益であるとすれば，一般的なプライバシー侵害の法的責任は民事責任が通例であって，刑罰を科すことはかなり例外的であると考えられる．従って，「通信の秘密」の保護法益と 179 条の罰則規定が，法的にはバランスを欠いているのではないか，との疑問についてどう考えれば良いであろうか？

1 章で述べたように，電気通信事業者の本来の役割は，預かった通信をノータッチ（hands -off）で運ぶことである．通信当事者が事業者はもちろん，公権力や他の第三者の介入を心配せずに，秘匿性を有する通信が行えることが通信の社会的な機能・役割である．この通信の社会的機能・役割を保障するために，近代国家になってから「通信の秘密」が憲法上の基本的な権利として認められたと解釈できないであろうか？

すなわち，通信当事者以外の通信事業者や公権力を含む第三者に対して，通信にノータッチを保障する手法として，「（事業者の取扱中に係る）通信の秘密を侵してはならない」の規定を置いて、通信当事者以外の何人に対しても知得、窃用、漏えいを禁止する.[70]

これによって通信当事者のプライバシーなどを保護する．そしてこのことを通して，通信の社会的機能・役割を果たそうとすることが，「通信の秘密」の規定の本旨であって，「通信の秘密」を保護することの基本にあるのではないかと考えられないであろうか？

この解釈を是とするならば，上記の「業務の適正・合理的運用およびそれに対する社会的信頼」を，「通信の秘密」の保護法益であるとの解釈が妥当であると考えられる.

従って，「通信の秘密」の保護法益にプライバシーなどの個人的法益を超えた社会的保護法益が含まれるとすれば，プライバシー侵害などに対する法的責任としてはバランスを欠くと考えられる 179 条の刑罰規定は妥当であると考えられる.

また，通信サービスを担っている通信事業者の違反行為は重大なので，刑罰加重の規定を置くことも妥当であると考えられる.

「通信の秘密」の保護法益を上記のように解すれば，通信事業者が預かった通信をノータッチ（hands-off）で運ぶとの「通信の秘密」を長年遵守してきたことの理由が理解できる.

---

[70] 但し電気通信事業の従事者が，業務上の必要に基づき「知得」することは認められている.

6.3 「通信の秘密」の保護法益に関する憲法と法律レベルの位置関係

「法律レベルの内容は，前者（憲法）の趣旨を具体化するものであるというのが従来の一般的説明であり，それ以上に立ち入った説明はあまり見られなかった」[71] と指摘されていたが，以下のように，憲法と法律レベルの保護法益は異なっているとの解釈が適切のように考えられる.

石井[2013]は，「国家による侵害を問題とする憲法 21 条 2 項における通信の秘密と電気通信事業法における通信の秘密が同一の意義，同一の内容のものであると解する必然性は乏しい.」[72]と述べている。

また，曽我部[2016]は、「憲法上の保障は公権力による侵害からの保障であり，法律上の保障は通信事業者や第三者である私人による侵害からの保障も含む」[73] として，名宛人が異なると指摘している.

法律レベルでは，憲法の保護法益であるとされるプライバシーに加えて，電気通信業務ないし通信システムの適正かつ合理的な運用を行うことによる社会的信頼が保護法益であると考えられる.

すなわち法律レベルでは，電気通信の社会的機能・役割を重視した保護法益論を採っていて，経済社会活動および国民生活が大きくインターネットに依存して行われている現状を，反映しているものと考えられる.

7 「通信の秘密」の制限

「通信の秘密」の構成要件に該当する行為を行っても，通信当事者の有効な同意または違法性阻却事由がある場合は適法行為となる．まず、憲法上の保護に関する概括的な問題について述べる．ついで，有効な同意と違法性阻却事由について述べ，続いて権利制限に関する憲法論，違法有害情報の場合とインターネットサービスの安定的な提供の場合の「通信の秘密」の保護の制限の正当化根拠の違いについて考察する.

7.1 憲法上の「通信の秘密」の保護と法律による制限

「通信の秘密」は，「憲法第 3 章　国民の権利及び義務」 21 条 2 項後段に規定されている自由権に属する権利である.

憲法上の権利を制限する場合の本人同意に関しては，制限の正当化理由となる場合とならない場合がある.[74]

---

[71] 出典:前掲注68 p16

[72] 出典:前掲注69 pp123～124

[73] 出典:出典:曽我部真裕 [2016]「第 3 章 通信と放送」曽我部真裕・林秀弥・栗田昌裕『情報法概説』p49 弘文堂

[74] 例えば，身体の不可侵性（13 条）や不利益供述拒否権（38 条 1 項）については，本人同意の範囲内で自己に有利な利益を放棄してもよいと考えられるため，当該権利の制限が正当化される．一方奴隷的拘束の禁止（18 条）や拷問や残虐な刑罰の禁止（36 条）については，個人の尊厳に関わる重大事項のため，絶対的禁止とされている．たとえ本人の同意があっても制限は正当化しえない．出典:松本和彦［2016］「第3章 三段階審査の手法」前掲注67 p68 日本評論社

憲法における「通信の秘密」の保障が法律レベルで制限される例としては，4.1 の表 1 および 5.1 の表 2 にその例がある．加えて公権力の行為によって制限される例としては，2.1.3 で述べた法律がある．

7.2 有効な同意の原則と例外

7.2.1 有効な同意[75]

「有効な同意があるとは，原則として，通信の秘密を侵すことに対する認識，認容がある場合といい，個別具体的かつ明確な同意が必要であるとされている.」[76]

この有効な同意に関して，「ゼロレーティングサービスの提供に係る電気通信事業法の適用に関するガイドライン」を例にして，その考え方をみてみたい.[77]

ゼロレーティングサービスを提供するためには，①ゼロレーティングサービス利用者と非利用者を区別する必要があり，②利用者が対象コンテンツを利用している場合をデータ通信量にカウントしないために，他のコンテンツ利用と区別する，この二つの区別が必要である．

この区別を行うために，「通信の秘密」に該当する情報を，適法行為として利用する必要がある．ガイドラインの整理としては，①については正当業務行為として違法性が阻却される．しかし②については正当業務行為とは認められないので，②の情報を利用するためには，利用者に十分説明の上で，「個別具体的かつ明確な同意」が必要であるとしている．

このガイドラインでは，①では違法性阻却事由があると判断して「通信の秘密」に該当する情報の知得を認める，②では違法性阻却事由が認められない場合でも，「有効な同意」があれば，「通信の秘密」に該当する情報の知得を認める，との手順を踏んでいる．

従って，「有効な同意」は，「通信の秘密」に該当する情報の知得を，違法性阻却事由が認められなくとも，同意に基づいて認めるものであって，しっかりとした根拠のある同意であることが求められる．このため，「有効な同意があるとは，原則として，通信の秘密を侵すことに対する認識，認容がある場合といい，個別具体的かつ明確な同意が必要」とされているものと考えられる．

有効な同意については上記の考え方が採られているため，契約約款等における事前の包括同意のみでは，有効な同意ではない[78]とされている．

---

[75] 20 年改正電気通信事業法の成立に伴い，「電気通信事業における個人情報保護に関するガイドラインの解説」が改正された．この改正に合わせて，「同意取得の在り方に関する参照文書」が策定されている．（2020年2月）

[76] 出典：曽我部真裕［2020］「通信の秘密」『法学セミナー』2020年7月号 p66

[77] 総務省「ゼロレーティングサービスの提供に係る電気通信事業法の適用に関するガイドライン」pp15～16 2020年3月

[78]「通信当事者の有効な同意がある場合には、通信当事者の意思に反しない利用であるため，通信の秘密の侵害に当たらない．この点に関して，有効な同意とは，原則として，通信の秘密を侵すことに対する認識，認容がある場合をいい，通常は契約約款等に基づく事前の包括同意のみしかない場合を含まない．その理由として契約約款は当事者の同意が推定可能な事項を定める性質のものであり，通信の秘密の利益を放棄させる内容は，通常その性質になじまないこと，事前の包括同意は将来の事実に対する予測に基づいて行われることから対象・範囲が不明確になる」ためとされている．出典「電気通

しかし，サイバー攻撃への対処策を検討する「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」の第一次から第三次のいずれのとりまとめにおいても，包括同意が認められている事例がある．

それぞれの事例で包括同意が「有効な同意」と認められた理由としては，同研究会のとりまとめでは「インターネットサービスの通常の利用者であれば，電気通信事業者が『通信の秘密』に該当する情報を利用することを許諾することが想定し得る」[79] からであると説明されている．

この説明は、「有効な同意」とは「個別具体的かつ明確な同意」であるとの基本原則からみると，かなりあいまいな正当化の理由であるように考えられる．というのも，「通常の利用者であれば想定される」ということが実証されているわけではないからである．

しかし包括同意を認めたのは，①当該対策を実行することが，サイバー攻撃対策として有効性が高く，かつ利用者を守ることになるため，実施すべきとの判断があること，② どのような場合にそれぞれの対策を実行するかを，契約約款に記載することで，利用者の同意が得られやすくなる[80]，との判断に基づいて包括同意を「有効な同意」として認めたのではないかと推測される．

7.2.2 包括同意が認められなかった事例

4.2 で分析した,海賊版対策の検討会議では，ブロッキング以外の対策の一つとして「アクセス警告方式」[81] についても提案されていた．この経過を受けて，総務省では 2019 年 4 月からの「インターネット上の海賊版サイトへのアクセス抑止方式に関する検討会」において，この方式をネットワーク側で，包括同意に基づいて実施することの可否について検討が行われた．同年 8 月に報告書が公表されたが，結論としては包括同意が「有効な同意」とは認められなかった．

検討会では、ISP が利用者のすべてのアクセス先をチェックすることを許容するかどうかのアンケート調査が行われたが，許容するとする割合は50％に満たない結果となった．このため包括同意を「有効な同意」として実施することは，困難であると結論づけられた．

7.3 違法性阻却事由

「刑法第7章 犯罪の不成立及び刑の減免」では、犯罪の構成要件に該当する行為を行

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」p10 2018年

[79] 出典:「電気通信事業におけるサイバー攻撃等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」p20 2014年

[80] 例えば「C&C サーバ等との通信の遮断」の事例では、少なくとも契約約款において規定すべき内容として、検知を行うこと, C&C サーバ等へのアクセスに係る通信の検知の目的，検知の時期，検知の対象となる情報の範囲，事後的に同意内容を変更できる（設定内容を変更できること）の5項目が挙げられている.出典:前掲注80 p21

[81]「アクセス警告方式」とは、「ユーザの同意に基づき,（中略） ISP がネットワーク上でユーザのアクセス先（海賊版サイト以外のサイトへのアクセスを含む）をチェックし,（中略） 海賊版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．出典:「インターネット上の海賊版サイトへのアクセス抑止方式に関する検討会報告書」p8 2019年8月

った場合でも、犯罪とはならない場合の規定を置いている．これには違法性阻却事由がある場合と，責任能力に問題がある場合の二つがある．

「通信の秘密」を侵害する行為の場合には，責任能力が問題になる場合は通常生じないので，違法性阻却事由，すなわち正当行為（35条），正当防衛（36条），緊急避難（37条）のいずれかが認められるかについて検討が行われている．認められた場合には，「通信の秘密」の構成要件への侵害行為でも適法行為となる．

まず法令に従う場合および正当業務行為に該当する場合は，正当行為に該当する．正当業務行為が認められるのは，電気通信役務の円滑な提供を果たす見地から，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ことが必要であるとされている．[82]

この正当業務行為の事例としては，①電気通信事業者が課金・料金請求目的で，顧客の通信履歴を利用する行為，②ISP がルータで通信のヘッダ情報を用いて経路を制御する行為等の通信事業を維持・継続する上で必要な行為，③ネットワークの安定的運用と認められる行為（大量通信に対する帯域制御等） が挙げられている．[83]

次に正当防衛の成立要件は，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，③やむを得ずにした行為の三つの条件を全て満たすことである．また緊急避難の成立要件は，①現在の危難の存在，②法益の権衡，③補充性の三つの条件を全て満たすことである．[84]

7.4 違法有害情報等の場合およびインターネットサービスの安定的提供の場合の「通信の秘密」の制限の正当化根拠

7.4.1 違法有害情報等の場合の正当化根拠

違法有害情報等に関する「通信の秘密」の制限事例については，4．1表1の通りであるが，どのような場合に「通信の秘密」を保護し，どのような場合に「通信の秘密」の制限を認めるのかについては，「通信の秘密」の保護の制限とその制限によって救われる法益の比較を行う手法によって行われている．[85]

インターネット上では多くの人が情報発信している．また多くの人が，情報発信した「表現内容」にアクセスしている．この「表現内容」の中には，権利侵害情報が含まれてい

---

82 出典：前掲注79 p11

83 出典：「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」第二次提言 p14 2010年

84 上記の「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とりまとめ（一次から三次まで）」においては、この三つの違法性阻却事由を根拠にして，「通信の秘密」の保護を制限する様々なサイバー攻撃対策が認められている．またこのとりまとめを受けて，電気通信事業関係 5 団体によって「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」が策定されていて，電気通信事業者はこのガイドラインに従って，業務運営を行っている．

85 表現の自由を制限する場合は，まず「形式的正当化としての法律保留の原則から，法律によるか，または法律に基づくことが必要である．」また実質的正当化としては，「判例では，（中略）制限の正当化の判断枠組みとして利益衡量論を採用している」とされる．出典：前掲注67 p239

るが，4．4で述べたようにプロバイダ責任制限法では，権利侵害情報によって権利を侵害されたとする者（被害者）の救済方法として，送信防止措置(3条) と発信者情報開示を求める方法（4 条）の二つが規定されている．

権利を侵害されたとする者（被害者）は、直接権利侵害者に対して法的責任を問うことが本来の方法である．しかしインターネット上では,情報発信者を特定することは困難であるため，事業者に対して関与を求めることによって，被害の回復を図ることになる．

送信防止措置（3条）および発信者情報開示（4条）においては，（名誉毀損などの）権利を侵害されたとする者（被害者）と，その書込みを行った者の「表現の自由」のどちらを優先するかについては，二者択一の関係にあると考えられる．

しかしこの二つには違いがある．すなわち発信者情報は,「通信の秘密」の保護対象である通信の構成要件であり,「電気通信事業者の取扱中の通信」によって，事業者が知得した情報である．従って発信者情報開示は，通信メディアとしてのインターネットに関する問題である．

一方，送信防止措置の場合は,「取扱中の通信」から離れて，多くの人がアクセスできるサーバ等に収納されている「表現内容」であり，表現メディアとしてのインターネットに関する問題である。

特定電気通信役務提供者（定義は同法2条3号）は、権利を侵害されたとする者（被害者）と権利侵害者との利害対立に関しては，当事者ではなく，またこれに関与する業務運営上のインセンティブはない．しかしインターネットが表現メディアでもために,「媒介者の責任」の役割[86]を果たすことが求められている．

7.4.2　インターネットサービスの安定的提供の場合の正当化根拠

インターネットサービスの安定的提供のために，5．1表2にあるように，電気通信事業者が「通信の秘密」を制限することが認められている．前7．4．1の違法有害情報の場合には,「通信の秘密」の保護と「通信の秘密」の制限の判断が二者択一であるのとは異なり，インターネットサービスの安定的提供の場合には,「通信の秘密」の保護と「通信の秘密」の制限の関係は二者択一の関係ではない．ここでは，インターネットサービスの安定的提供に関する問題の中で，サイバー攻撃の場合について考察する．

「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イン」では,「通信の秘密」を制限する多くのサイバー攻撃対策が認められている．

この違法性阻却事由の有無の判断は，当該サイバー攻撃対策の目的の正当性，行為の必要性および手段の相当性の三つによっている.[87]

---

86 この「媒介者の責任」について、成原はさまざまな視点から論じている．以下を参照．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』Vol．80．同［2015］「情報流通の媒介者と表現の自由」『Nextcom』Vol．21 2015 Spring

87 基本権（権利）の制限が憲法上認められるかについての審査手法の一つとして，目的・手段の図式によって権利制限の実質的正当化の審査が行われている．この審査では，目的審査（制限する正当な目的があるか），手段審査（手段として正統性があるか）および比例原則（手段が目的と適切な関係にあるか）の三段階の審査が行われる．出典:．前掲注75 pp74～78．この審査手法が，サイバー攻撃対策の違法性阻却の有無の判断における目的の正当性，行為の必要性および手

第二次とりまとめにおいて，サイバー攻撃への対策として正当業務行為であると認められた，「新たな DDoS 攻撃である DNSAmp 攻撃の防止」を例にして考察してみたい．

第二次とりまとめでは，この攻撃を防止するためには，「全ての通信の宛先 IP アドレス及びポート番号を常時確認して，該当する通信をブロックする必要がある．」と述べられているが，この常時確認は「通信の秘密」の侵害行為に該当する．

しかし，この常時確認を行うことによって，DNSAmp 攻撃が防止できるとすれば，インターネットサービスの安定的提供に役立つことになり，「通信の秘密」を保護することにもなる．このように，サイバー攻撃対策においては，「通信の秘密」を制限する行為が，「通信の秘密」を保護する行為でもあるとの関係にある．

7.4.3 「通信の秘密」の保護法益および「通信の秘密」の制限の正当化根拠

6章において「通信の秘密」の保護法益を考察したが，憲法の保護法益に加えて、今日の社会経済活動が大きくインターネットに依存している状況を踏まえて，法律レベルではインターネットサービスの安定的提供およびこれに対する社会的な信頼が「通信の秘密」の保護法益と解することが適切ではないかと述べた．また，法 1 条においては，「電気通信役務の円滑な提供を確保する」ことが，法目的として掲げられている．

前 7.4.2 で述べたことを考えると，「インターネットサービスの安定的提供およびこれに対する社会的な信頼」というのは，また「通信の秘密」の制限の正当化根拠でもあると考えられる．このように「インターネットサービスの安定的提供およびこれに対する社会的な信頼」が，「通信の秘密」の保護であるとともに「通信の秘密」の制限であることは，一見すると矛盾しているように考えられる．

しかし，サイバー攻撃における「通信の秘密」の制限が，前述したように「通信の秘密」を保護することにもなるとの本稿の解釈から考えれば，「インターネットサービスの安定的提供およびこれに対する社会的な信頼」が，一方で「通信の秘密」の保護法益であり，他方で，「通信の秘密」の制限の正当化根拠であることは，むしろ当然の帰結ではないかと考えられる．

以上の考察からいえることは，違法有害情報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，「通信の秘密」を制限することは共通している．しかし前者の場合は「通信の秘密」の保護と「通信の秘密」以外の権利の保護のどちらを優先するかとの二者択一の関係であるのに対して，後者の場合は「通信の秘密」を制限する行為が「通信の秘密」の保護にも役立つということになっているという点において，大きな違いがあると考えられる．

以上の考察によって，「通信の秘密」に関する電気通信事業者の役割は，預かった通信に関してノータッチ（hands-off）から，インターネットにおいては関与が求められまたは認められるようになっていて，大きく変質していることが浮き彫りになったと考えられる．

「通信の秘密」 の問題を，再度サイバーセキュリティの観点から考えると，防御力，抑

段の相当性に対応するものであることが読み取れる

止力，状況把握力を強化する政策・法制度が必要であり，またこれを同等もしくはそれ以上に技術面および管理面での強化を図ることによって，インターネットサービスの安定的提供が可能になり，「通信の秘密」の保護が可能になると考えられる．

8 「通信の秘密」の保護法益（再説）

7 章における考察を考慮すると，インターネット利用においては，「通信の秘密」の保護はそれほど重要ではなくなったと考えるべきであろうか？ いやそうではなく，「通信の秘密」は，インターネット時代においても依然として重要な価値を有していると考えられるので，本章ではこの問題について考察してみたい．

8.1 EU-Japan Adequacy Decision

EU 委員会は，2019 年 1 月に日本に対して個人情報保護に関する十分性認定の決定（Adequacy Decision）を行った．この決定文書において，十分性認定のために行なわれた調査結果が述べられている．1 章の Introduction に続いて，2 章では民間部門のデータ処理に関する法律の概要が述べられている．

次いで 3 章において，政府部門の個人データへのアクセス（government access）に関する法制度について述べられている．まず憲法の関係条文として 35 条（住居侵入・捜索・押収に対する保障）について言及するとともに，21 条 2 項の「通信の秘密」（the secrecy of all means of communication）は，公共の福祉を根拠（public interest grounds）とする立法によってのみ制限されると述べられている．

加えて，法 4 条の規定内容および法 179 条の規定についても述べられている．またこれらの規定は，利用者の同意又は刑法の明確な例外規定（the explicit exemptions from criminal liability under the Penal Code）による以外は，通信情報の開示（disclosure of communications information）を禁止していると解釈されると述べられている．この十分性決定文書においては，「通信の秘密」の規定は個人情報（データ）保護との関わりの文脈で述べられている．

また，刑法による電子情報の押収は，令状に基づくか又は任意開示要請によって認められること，および通信傍受法について述べられている．さらに日本では強制手続きは犯罪捜査に限られていて，国家安全保障の理由での強制手続きによる情報取集を認める法律はないとも述べられている．[88] [89]

---

[88] 出典：“Commission Implementing Decision of 23.1.2019 pursuant to Regulation(EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information”

[89] 2013 年のエドワード・スノーデンが，NSA の秘密裡に行なわれていた活動を暴露したことを契機として，EU−米国間でセーフ・ハーバーの見直し交渉が行われた．この交渉においては，EU の問題関心は米国政府による個人データの収集問題（government access）に集中していた．この交渉の結果 2016 年にプライバシー・シールドが発効したが，内容としては政府アクセスの内容が大宗を占めていた．このことを背景にして，EU−日本間の十分性認定においても，政府アクセスに関する法制度の在り方が，重要な判断要素であったように考えられる．なお，エドワード・スノーデンが暴露した内容および EU 米国

8.2 普遍的価値を守るための「通信の秘密」の位置づけ

電話利用において，「通信の秘密」の主な侵害事例は2．2．3で述べた通りであり，事例は少ない．一方インターネット利用においては，これまで述べてきたように，「通信の秘密」の構成要件に対する侵害行為が、同意または違法性阻却事由があることを理由にして適法とされる事例がみられるようになっている．特に，サイバーセキュリティ分野での事例が多くなっている。

これらの事例を一見すると，「通信の秘密」の保護のレベルが低下しているような印象を受けるかもしれない．しかし「通信の秘密」の保護は，以下の 3 点の理由から依然として重要な法的価値であると考えられる．

(1) 一つ目の理由は，8.1 でとり上げた EU-Japan Adequacy Decision でおいて，その認定根拠の一つとして憲法および電気通信事業法に「通信の秘密」が規定されていることが明記されていることである．今後も「十分性認定」を維持しようとするならば，現行の「通信の秘密」は不可欠な規定であると考えられる．

(2) 二つ目の理由は，プライバシーなどが「通信の秘密」の保護法益であることと関係する．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.」と述べ，個人情報保護における「通信の秘密」の規定の重要性を指摘している.[90]

もっとも，この「表現の自由とプライバシーの基盤がそれほど強くない」との宍戸発言が，これらの権利に対する日本人の意識が強くないという意味の発言なのか，これらの権利を守る法制度がそれほど強固ではないとの発言なのかは，文面では分からない．しかしいずれにしても，それほど強くない権利意識，またはプライバシーや表現の自由に係る法制度の不十分さを，「通信の秘密」の規定が補っているとの認識を示したものと考えられる．

また成原[2018] は，「通信の秘密は，我が国特有の『ガラパゴスなルール』ではなく，それが仕える価値は普遍的」であると指摘している．その理由として「通信の秘密」が憲法上明記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」こと，また欧米での「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リスクへの着目」の議論動向を挙げている.[91]

間のプライバシー・シールド交渉および内容については，以下を参照．林紘一郎・田川義博［2016］「セ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』 8 号 pp21～29．石井夏生利［2017］『新版 個人情報保護法の現在と未来』pp297～353 勁草書房

90 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れど 赤松健さん，宍戸常寿さん，別所直哉さん」

91 出典：成原慧「SOPA/PIPA 法案をめぐる米国の議論と我が国への示唆」 知的財産戦略本部海賊版タスクフォースヒアリング資料 p13 2018年9月13日．なお，「メタデータの収集・分析によるプライバシー侵害リスク」の問題は，主に GAFA

宍戸と成原の議論は，欧米ではプライバシーや表現の自由の問題として議論されている問題が，日本においては「通信の秘密」の問題として一部議論されていることを示唆しているように考えられる．しかし本稿で考察した「通信の秘密」の保護法益を考えれば、同一のテーマを欧米と日本では異なる用語を用いて議論しているものと考えられる．

従って，これらの普遍的価値に関する法制度のハーモナイゼーションが検討課題になると考えられる．1989 年のベルリンの壁の崩壊と 1990 年のソビエト連邦の解体によって，資本主義対社会主義（共産主義）の競争が終わり，今後は資本主義同士の制度間競争が重要になるとの指摘が当時なされていた．（もっとも，現在は自由資本主義対権威資本主義，または民主主義対（強圧的）覇権主義の競争が大きな政治的課題になっている．）

この文脈で考えれば，個人情報の保護と活用に関する法制度の良否が，個人情報保護などの権利の保障レベル，各国産業の国際競争力および国民生活の質を左右することになると考えられる．このため成原の指摘している「サイバーセキュリティ」も含めて，この観点から「通信の秘密」の保護ないし価値について，政策・法制度だけではなく技術面や管理面も併せて考察を深めていくことが重要であると考えられる．

(3) 三つ目の理由は，Society5.0 では情報通信ネットワークシステムの高度化および安全で安定的なサービス提供が，社会経済活動，国民生活および安全保障にとって死活的な重要性を有していることが挙げられる．

サイバーセキュリティの観点からは，「通信の秘密」を制限した対策をとることが，Socity5.0 において致命的な重要性を有する情報ネットワークシステムの安全で安定的な提供につながるものと考えられる．従ってサイバーセキュリティにおいては，「通信の秘密」の制限が「通信の秘密」の保護と重複性ない両義性を有することが理解できると考えられる．

2.2.5 で述べたように，「電気通信事業者の取扱中の通信」の保護の対象領域は，サイバーセキュリティの対象範囲よりも狭い．しかし実際には，電気通信事業者がインターネッ

によるプライバシー侵害のリスク問題として議論されている．日本においても，公正取引委員会，経済産業省および総務省の合同検討を経て，「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律」（「デジタルプラットフォーム取引透明化法」）が，「2021 年 2 月に施行され，本格運用のフェーズに入る」．また「取引デジタルプラットフォームを利用する消費者の利益の保護に関する法律」（「デジタルプラットフォーム消費者利益保護法」）が 2021 年 4 月に成立し，一つの大きな節目を迎えている．」と指摘されている．出典：安平武彦［2021］「デジタルプラットフォームをめぐる規制の到達点と実務（1）」『NBL』No.1194（2021.5.15）p33．以下も参照．北島洋平・安平武彦・岡本健太・佐久間弘明［2020］「特定デジタルプラットフォームの透明性及び公正性の向上の法律の概要」『NBL』No.1174（2020.7.15）．またプラットフォームに関しては多くの文献があるが，以下も参照．森亮二［2020］「プラットフォームの法的責任と法規制の全体像」，別所直哉［2020］「プラットフォーム規制とイノベーション」『Jurist』May 2020 / Number1545.

トサービスの安定的提供のために，「通信の秘密」を制限することが、自らが運営管理する通信システムを守ることに加えて，その対象範囲外である利用者のクラウドを含む情報システムおよびその中に蓄積されている情報を保護することにもなる.

従って，サイバーセキュリティ分野において「通信の秘密」を制限することが、「通信の秘密」の保護にもなるとともに，情報通信ネットワークシステム全体のサイバーセキュリティにプラスの効果を生むことを再度確認しておきたい.

9 通信ネットワークの未来と法の役割

9.1 通信ネットワークをめぐる技術革新と電気通信事業法の在り方

この数年，総務省情報通信審議会「電気通信事業分野における競争ルール等の包括的検証に関する特別委員会」に設置された 3 つの WG が，ネットワーク中立性研究会やプラットフォーム研究会などとも連携して精力的な検討を行った.

この特別委員会における包括的検証という意欲的なテーマ設定の目的は，①2030年に至るネットワーク構造および市場構造の変化の方向性を探ること，② この変化が提起する，電気通信政策・法制度に対して与える影響を予め検討すること，③この影響に対処するための当面および中長期の課題を抽出することであると考えられる.

この包括的検証の取組は，バックキャスティングの手法によって，先手の政策・法制度の検討を行おうとするものであると考えられる.[92]

これらの検討の具体的成果として，長年の懸案であった国外事業者に対する電気通信事業法の適用に関する 20 年改正電気通信事業法の成立などが挙げられる．本節ではこの包括的検証の中から，ネットワーク構造および市場構造の変化が，電気通信事業法の規律の在り方へどのように影響するのかを探ってみたい.

まず通信ネットワークに関する技術革新によって，いままでの設備，機能，サービスを一体的に電気通信事業者が提供していた形態が崩れ，「電気通信回線設備を自ら設置することなく」，仮想化管理（ネットワーク・オーケストレーション） やネットワーク・スライシングサービスなどを行う，「機能を活用する主体」の登場が想定されている．このなかには，OTT事業者がネットワークサービスを提供する動きも含まれるとみられる.

このように設備を設置する主体と機能を活用する主体の分離が進んだ場合に，現行ルールではその主体・サービスの位置づけが明らかではない．このため，「仮想化技術等の導入によるイノベーション・新ビジネスの創出も考慮しつつ，参入規律の在り方，安全・信頼性の確保の在り方，関係主体が多種多様となることを踏まえた利用者保護等の在り方等を中心」にした政策課題が設定されている.

一方で，NTT が提唱する IOWN 構想では，「設備」と「サービス/機能」の融合が進

[92] この取り組みは，先手の政策・法制度の検討であると評価はできる．しかし次9．2では，産業分野毎に事業者の行為をあらかじめ規制するタイプの法（規制的な法，業法）が，イノベーションのスピードが速くかつ不確実性が増している社会では，その有効性を失うとの指摘がなされている．また，ルールベースからゴールベースの法規制への移行も提唱されているなかで，業法である電気通信事業法自体の在り方が今後問われることになる.

展すると想定される，とも述べられている.[93]

このようなネットワーク構造および市場構造の変化が，電気通信事業法に与える影響としては，1）まず法の適用範囲が多種多様な参入事業者にどこまで及ぶのかの問題がある. 2）次いで，設備とりわけ回線設備に着目した法体系が今後も維持できるのか，または維持すべきかとの問題もある．3）さらに，法２条の「電気通信」などの定義を維持できるか，または維持すべきかとの問題も想定し得る.

1）の問題に関しては，20 年改正電気通信法では、国外事業者を法の規律対象とすることになったが，ネットワーク構造および市場構造が変化するなかで，OTT 事業者などが欧米の規制体系を根拠に電気通信事業法の規制対象となることに難色を示すことも想定される.

2）の問題に関しては，現行の「設備」に着目した規律から，サービスなり機能なりの他の指標に依拠する法体系への大転換も，検討せざるを得ないことも想定される.[94]

3）の問題は，「通信の秘密」の規律の基礎となる「通信」自体の変質であり，そもそも「通信の秘密」の対象となる「通信」はどの範囲なのかについての検討が迫られることも想定し得る.

現在のインターネット上では，３．２．２で引用した「秘匿性のある特定当事者間の通信」が占める割合は限定的であり，表現行為のための通信はもちろん，クラウド利用，IoT などとのマンツーマシーン，マシーンツーマシーンの情報流通が大宗を占めることになると考えられる.

この状況において，多賀谷[1995]は，インターネット上のコンピュータ間通信におけるデータの保護は，プライバシー保護というよりは営業秘密の保護の問題であり，通信セキュリティにおいては，通信の秘密は一要素であって，それと共に通信エラーのないこと，相手方への送信確認および受信確認などが求められる． 従って「通信の秘密」は，秘匿性を有する当事者間の通信に限定されるべきと指摘している.[95]

9.2 Society 5.0 におけるガバナンスにおける法の役割

経済産業省に 2019 年に設置された「Society 5.0 における新たなガバナンスモデル検討会」は，2020年７月に「Governance Innovation：Society5.0の実現に向けた法とアーキテクチャのリ・デザイン」報告書（以下、第１弾報告書）を公表した.

次いで2021年７月に，「Governance Innovation Ver.2：アジャイル・ガバナンスのデザイ

---

93 出典:「電気通信事業分野における競争ルール等の包括的検証 最終答申」p40～46，p62～67 情報通信審議会 2019 年 12 月 17 日

94「電気通信役務か電気通信役務類似の役務かの区分が無意味化．設備に着目して規律を行う電気通信事業法の存在意義が問われる可能性.」との指摘もある．出典：曽我部真裕［2018］「2030 年のネットワークの規律のあり方についての憲法的考察」電気通信事業分野における競争ルール等の包括的な検証に関する特別委員会・主査ヒアリング資料 p3 2018年11月12日

95 出典：多賀谷一照『行政とマルチメディアの法理論』pp109～133，pp189～206．なお，多賀谷説が説かれたのは1995年であって，現在のインターネットの利用状況を踏まえてのものではないことに注意が必要である．この時期に上記の指摘を行ったその先見性に驚くとともに，敬意を表したい.

ンと実装に向けて」と題する報告書（以下、第 2 弾報告書）を公表した．Society5．0における変化の中で，前9．1の問題の基礎にあると考えられる法自体の機能・役割の変化について探ってみたい．

上記の報告書では，ガバナンス手法として，ローレンス・レッシグの法，市場，社会規範およびアーキテクチャの 4 類型に依拠した検討を行っている．そして従来型の「ルースベースの法規制」の見直しが，提言されている．「ここで想定されているのは，産業分野ごとに事業者の行為をあらかじめ規制するタイプの法（規制的な法，業法）」である．[96]

このルールベースの法規制を見直す理由は，法規制を中心とする従来型のガバナンスモデルでは，イノベーションのスピードに追い付くことが困難と想定されるためである．すなわち従来型の法規制は，「国が『あるべきルール』を業界ごとに特定することを前提としているが，CPS（cyber physical system）を基盤とする社会においては，（中略）具体的な規制範囲や行為義務を定めることが困難である．仮にそれを定めたとしても，法がイノベーションによって生ずるリスクをコントロールできなかったり，逆にイノベーションを阻害」[97]する可能性があるとしている．

このルールベースの法規制に代わり提言されているのが，「ルール形成・モニタリング・法執行の各段階で，（中略） 人権・公正・安全等を保障し実現する『ゴールベースの法規制』」[98] である．

この新しいゴールベースの法規制では，最終的に達成されるべき価値を示して，その価値を実現するための法規制内容に変えることが提言されている．このように報告書ではSociety5．0においては先を見通すことが従来よりも困難になり，リスク管理・不確定性の視点から，大きな変化に対応すべく，幅広くかつ深いレベルでの変革が提言されている．

提言内容については第 1 弾および第 2 弾報告書を参照願いたいが，報告書ではガバナンス主体が従来の国主体から拡散すること，およびガバナンス手法がレッシグの提唱する4類型への多彩化させることを提言するとともに，ゴールとしては基本的人権，公正競争，民主主義，環境保護などを挙げている．

また稲谷は 「法の支配の将来像」として，ハードローよりもソフトローに、司法判断より協調的法執行によりウエイトが置かれる可能性を想定している．その場合に，ソフトローの形成・執行段階における高いアカウンタビリティと手続き保障が重要な意味を持つ．また技術的権力（筆者注：アーキテクチャのこと） の影響力増大に対しては，コードやアーキテクチャの構築主体に対するアカウンタビリティと，透明性の高い情報開示制度が必要であると指摘している．[99]

---

96 出典：第 1 弾報告書 巻頭言 宍戸常寿 「Society5．0時代のガバナンスと法」 p．iv

97 出典：第 2 弾報告書 p66

98 前掲注97 p．v

99 出典:前掲注98 p73．稲谷龍彦執筆のコラム．なお以下も参照．稲谷龍彦[2021]「Society5.0 における刑事制裁の役割」『法学セミナー』2021/3 no.794 同「人工知能搭載機器に関する新たな刑事法規制について」『法律時報』91巻4号

一方で，「法律の密度を向上させるべきではないか．（中略）例えば，通信の秘密については，ごく簡単な事業法の条文のもとで，膨大な問題群が処理されていて整理が求められている状況になっている．（中略） e プライバシー規則案では原則と例外の基本的内容が書き込まれていて，（中略） 日本法もこのような形で基本的な構造は法律で定めるべきではないか．」

これらの報告書の提言のように，法・市場・規範・アーキテクチャの活用とルールベースの法からゴールベースの法へ移行することについての合意形成，およびルールベースの法の規定内容と形式の具体化が，どのようなプロセスを経て，いつ頃明確になるかは，現時点明らかではない．

また AI・IoT の導入・活用が，従来のガバナンスや法の在り方に大きな影響を及ぼすとの議論が活発に行われていて，法体系の根本からの問い直しが迫られる時期が近づいているようにも考えられる．またこの問い直しの必要性が，特に刑事法分野の実体法と手続法において高く，他の法分野よりも先行するようにも考えられる．

今後のガバナンスと法の在り方の基本的検討に当たっては，個別の専門領域を超えた視座のもとで，全体構想を描き具体化する試みが，どのような主体のリーダーシップの下で，行われていくのかが注目される．[100]

[電気通信事業法 ：本文で表記した条文]

（定義）
第二条 この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
一 電気通信 有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けることをいう。
二 電気通信設備 電気通信を行うための機械、器具、線路その他の電気的設備をいう。
三 電気通信役務 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ことをいう。
四 電気通信事業 電気通信役務を他人の需要に応ずるために提供する事業（放送法（昭和二十五年法律第百三十二号）第百十八条第一項に規定する放送局設備供給役務に係る事業を除く。）をいう。
五 電気通信事業者 電気通信事業を営むことについて、第九条の登録を受けた者及び第十六条第一項の規定による届出をした者をいう。
六 電気通信業務 電気通信事業者の行う電気通信役務の提供の業務をいう。

（検閲の禁止）
第三条 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）
第四条 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。

（電気通信事業の登録）
第九条 電気通信事業を営もうとする者は、総務大臣の登録を受けなければならない。ただし、次に掲げる場合は、この限りでない。（後略）

との指摘もある．出典：前掲注95 p11

[100] この基本からの問い直しに当たっては，林が説くように「情報の特質と法の在り方」，「法的規律の対象としての情報」など，情報および情報法に関する基本的な洞察を踏まえて，検討されることが望まれる．
出典：林紘一郎［2017］『情報法のリーガル・マインド』勁草書房

第十条 前条の登録を受けようとする者は、総務省令で定めるところにより、次の事項を記載した申請書を総務大臣に提出しなければならない。
一 氏名又は名称及び住所並びに法人にあつては、その代表者の氏名
二 外国法人等（外国の法人及び団体並びに外国に住所を有する個人をいう。以下この章及び第百十八条第四号において同じ。）にあつては、国内における代表者又は国内における代理人の氏名又は名称及び国内の住所 （後略）

（電気通信事業の届出）
第十六条 電気通信事業を営もうとする者（第九条の登録を受けるべき者を除く。）は、総務省令で定めるところにより、次の事項を記載した書類を添えて、その旨を総務大臣に届け出なければならない。
一 氏名又は名称及び住所並びに法人にあつては、その代表者の氏名
二 外国法人等にあつては、国内における代表者又は国内における代理人の氏名又は名称及び国内の住所 （後略）

（業務の停止等の報告）
第二十八条 電気通信事業者は、第八条第二項の規定により電気通信業務の一部を停止したとき、又は電気通信業務に関し通信の秘密の漏えいその他総務省令で定める重大な事故が生じたときは、その旨をその理由又は原因とともに、遅滞なく、総務大臣に報告しなければならない。

（業務の改善命令）
第二十九条 総務大臣は、次の各号のいずれかに該当すると認めるときは、電気通信事業者に対し、利用者の利益又は公共の利益を確保するために必要な限度において、業務の方法の改善その他の措置をとるべきことを命ずることができる。
一 電気通信事業者の業務の方法に関し通信の秘密の確保に支障があるとき。 （後略）

（秘密保持義務）
第百十六条の四 認定送信型対電気通信設備サイバー攻撃対処協会の役員若しくは職員又はこれらの職にあつた者は、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を漏らしてはならない。
（適用除外等）
第百六十四条 この法律の規定は、次に掲げる電気通信事業については、適用しない。
一 専ら一の者に電気通信役務（当該一の者が電気通信事業者であるときは、当該一の者の電気通信事業の用に供する電気通信役務を除く。）を提供する電気通信事業
二 その一の部分の設置の場所が他の部分の設置の場所と同一の構内（これに準ずる区域内を含む。）又は同一の建物内である電気通信設備その他総務省令で定める基準に満たない規模の電気通信設備により電気通信役務を提供する電気通信事業
三 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ことなく提供する電気通信事業
（中略）
3 第一項の規定にかかわらず、第三条及び第四条の規定は同項各号に掲げる電気通信事業を営む者の取扱中に係る通信について、第百五十七条の二の規定は第三号事業を営む者について、それぞれ適用する。
4 認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号に掲げる業務が電気通信事業に該当しない場合においても、認定送信型対電気通信設備サイバー攻撃対処協会が行う同号ロの通知は、電気通信事業者の取扱中に係る通信とみなして第三条及び第四条の規定を適用し、認定送信型対電気通信設備サイバー攻撃対処協会が行う同号に掲げる業務に従事する者は、電気通信事業に従事する者とみなして同条第二項の規定を適用する。

5　認定送信型対電気通信設備サイバー攻撃対処協会が取り扱う第百十六条の二第二項第二号ロの通信履歴の電磁的記録は、電気通信事業者の取扱中に係る通信とみなして第三条及び第四条の規定を適用し、認定送信型対電気通信設備サイバー攻撃対処協会が行う同号に掲げる業務に従事する者は、電気通信事業に従事する者とみなして同条第二項の規定を適用する。

（報告及び検査）
第百六十六条　総務大臣は、この法律の施行に必要な限度において、電気通信事業者若しくは媒介等業務受託者に対し、その事業に関し報告をさせ、又はその職員に、電気通信事業者若しくは媒介等業務受託者の営業所、事務所その他の事業場に立ち入り、電気通信設備（電気通信事業者の事業場に立ち入る場合に限る。）、帳簿、書類その他の物件を検査させることができる。
（後略）

（法令等違反行為を行つた者の氏名等の公表）
第百六十七条の二　総務大臣は、電気通信役務の利用者の利益を保護し、又はその円滑な提供を確保するため必要かつ適当であると認めるときは、総務省令で定めるところにより、この法律又はこの法律に基づく命令若しくは処分に違反する行為（以下この条において「法令等違反行為」という。）を行つた者の氏名又は名称その他法令等違反行為による被害の発生若しくは拡大を防止し、又は電気通信事業の運営を適正かつ合理的なものとするために必要な事項を公表することができる。

第百七十九条　電気通信事業者の取扱中に係る通信（第百六十四条第三項に規定する通信並びに同条第四項及び第五項の規定により電気通信事業者の取扱中に係る通信とみなされる認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号ロの通知及び認定送信型対電気通信設備サイバー攻撃対処協会が取り扱う同項第二号ロの通信履歴の電磁的記録を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。
2　電気通信事業に従事する者（第百六十四条第四項及び第五項の規定により電気通信事業に従事する者とみなされる認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号又は第二号に掲げる業務に従事する者を含む。）が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。
3　前二項の未遂罪は、罰する。

第百九十条　法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、次の各号に掲げる規定の違反行為をしたときは、行為者を罰するほか、その法人に対して当該各号に定める罰金刑を、その人に対して各本条の罰金刑を科する。
一　第百八十一条　一億円以下の罰金刑
二　第百七十七条から第百七十九条まで、第百八十二条第二号又は第百八十五条から第百八十八条まで　各本条の罰金刑

引用/参照文献

[1] あきみち・空閑洋平 [2011]『インターネットのカタチ』オーム社
[2] 芦部信喜・高橋和之補訂『憲法 第 5 版』岩波書店
[3] 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
[4] 石井徹哉 [2013]「通信の秘密侵害罪に関する管見」『千葉大学法学論集』27 巻 4 号
[5] 稲谷龍彦「Society5.0 における刑事制裁の役割」『法律時報』91巻4号
[6] 宇賀克也・長谷部恭男 『情報法』有斐閣
[7] 上沼柴野「誹謗中傷と有害情報」『Jurist』February 2021 Number1554

[8] 海野淳史 [2018]「法律上の通信の秘密の『間隙』とその立法的解決」『情報通信学会誌』Vol.35 No.4
[9] 経済産業省 [2020]「Governance Innovation：Society5.0 の実現に向けた法とアーキテクチャのリ・デザイン」
[10] 経済産業省 [2021]「Governance Innovation Ver.2：アジャイル・ガバナンスのデザインと実装に向けて」
[11] 高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進会議 [2021]「デジタル社会の実現に向けた重点計画」
[12] 佐藤幸治 [2011]『日本国憲法』成文堂
[13] 阪本昌成 [1995]『憲法理論Ⅲ』成文堂
[14] サイバーセキュリティ戦略本部 [2021]「次期サイバーセキュリティ戦略」
[15] 宍戸常寿 [2013a]「通信の秘密」『季刊 企業と法創造』35 号 2013 年 2 月
[16] 宍戸常寿 [2013b]「通信の秘密に関する覚書」長谷部恭男・安西文雄・宍戸常寿・林知更（編）『現代立憲主義の諸相（下）』有斐閣
[17] 宍戸常寿 [2017]「円滑なインターネット利用環境の確保に関する検討会」第 1 回資料
[18] 宍戸常寿 [2018a]「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」インターネット上の海賊版対策に関する検討会議 第 4 回資料 4
[19] 宍戸常寿 [2018b]「中間とりまとめ（案）に対する意見」インターネット上の海賊版対策に関する検討会議 第 7 回 資料 11
[20] 宍戸常寿 [2021]「インターネット上の誹謗中傷問題」『Jurist February』2021 No.1554
[21] 清水真 [2017]「31 電話検証」『刑事訴訟法判例百選』
[22] 島田聡一郎 [2007]「第 1 章 リスク社会と刑法」長谷部恭男責任編集『リスク学入門 3』p10 岩波書店
[23] 自由民主党政務調査会 [2021]「新国際秩序創造戦略本部 中間とりまとめ」
[24] 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 2000 年 12 月 15 日号
[25] 曽我部真裕 [2013]「通信の秘密の憲法解釈論」『Nextcom』Vol.16 2013 Winter
[26] 曽我部真裕・林秀弥・栗田昌裕 [2016]『情報法概説』弘文堂
[27] 曽我部真裕 [2018]「2030年のネットワークの規律のあり方についての憲法的考察」総務省・電気通信事業分野における競争ルール等の包括的検証に関する特別委員会・主査ヒアリング
[28] 曽我部真裕 [2020]「通信の秘密」『法学セミナー』
[29] 曽我部真裕 [2021]「改正プロバイダ責任制限法の概要と成立の背景・経緯」『ビジネス法務』2021 年 8 月号
[30] 総務省 [2007]「郵便・信書便における通信の秘密」郵便・信書便制度の見直しに関する研究会
[31] 総務省 [2010]「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会第二次提言」
[32] 総務省 [2014a]「緊急時等における位置情報の取扱いに関する検討会 報告書」
[33] 総務省 [2014b]「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」

[34] 総務省［2018］「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」
[35] 総務省［2019a］「電気通信参入マニュアル[追補版]」2019 年 5 月 22 日最終決定
[36] 総務省［2019b］「インターネット上の海賊版サイトへのアクセス抑止方式に関する検討会報告書」
[37] 総務省［2019c］「電気通信事業分野における競争ルール等の包括的検証 最終答申」情報通信審議会
[38] 総務省［2020a］「ゼロレーティングサービスの提供に係る電気通信事業法の適用に関するガイドライン」
[39] 総務省［2020b］「インターネット上の誹謗中傷への対応に関する政策パッケージ」
[40] 総務省［2021a］「同意取得の在り方に関する参照文書」
[41] 総務省［2021b］「ICT サイバーセキュリティ総合対策 2021」
[42] 田川義博［2011］「情報セキュリティからみた東日本大震災」『情報セキュリティ総合科学』Vol. 3 情報セキュリティ大学院大学
[43] 多賀谷一照［1995］『行政とマルチメディアの法理論』弘文堂
[44] 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』（財）電気通信振興会
[45] 高橋則夫・松原芳博編［2012］『判例特別刑法』日本評論社
[46] 知的財産戦略本部・犯罪対策閣僚会議［2018］「インターネット上の海賊版サイトに対する緊急対策」
[47] 電気通信関係法コンメンタール編集委員会編［1973］『電気通信関係法詳解＜下巻＞』一二三書房
[48] 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
[49] 内閣府科学技術・イノベーション推進事務局［2021］「戦略的イノベーション創造プログラム（SIP）IoT 社会に対応したサイバー・フィジカル・セキュリティ研究開発計画」
[50] 内閣府等［2021］「インターネット上の海賊版に対する総合的な対策メニュー及び工程上について」
[51] 永野秀雄［2021］「バイデン大統領による大統領令第 14028 号『国家サイバーセキュリティの向上』『CICTEC Journal』2021.7 No.194
[52] 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』Vol. 80
[53] 成原慧［2015］「情報流通の媒介者と表現の自由」『Nextcom』Vol.21 2015 Spring
[54] 成原慧［2018］「SOPA/PIPA 法案をめぐる米国の論議と我が国への示唆」知的財産戦略本部海賊版タスクフォースヒアリング資料
[55] 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
[56] 林紘一郎［2017］『情報法のリーガル・マインド』勁草書房
[57] 林紘一郎［2021］「研究技術情報のセキュリティ管理」『情報セキュリティ総合科学』Vol. 13 2021 情報セキュリティ大学院大学
[58] 丸橋透［2021］「媒介者の責任」『Jurist』February 2021 Number 1554
[59] 安平武彦［2021］「デジタルプラットフォームをめぐる規制の到達点と実務(1)」『NBL』No.1194 (2021.5.15)

[60] 山郷・小林・岡辺 [2020]「令和 2 年改正電気通信事業法の実務対応」『NBL』No.1180（2020.10.15）
[61] 立案担当者解説 [2020]「電気通信事業法及び日本電信電話株式会社等に関する法律の一部を改正する法律」総務省 『情報通信政策研究』4 巻 1 号
[62] 若江雅子 [2021]『膨張 GAFA との闘い』中央公論新社
[63] 渡辺康行・宍戸常寿・松本和彦・工藤達郎 [2016]『憲法 I 基本権』日本評論社
[64] Commission Implementing Decision of 23.1.2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information"
[65] IISS [2021] "Cyber Capabilities and National Power: A Net Assessment"