# サイバーセキュリティにおけるバルクデータの意義

林紘一郎* 田川義博†

**概 要**

俗称イスラム国の登場などによって，事前にマークされていない犯人によるテロが頻発するようになったため，シギント活動においても，対象を限定して収集する「特定データ」ではなく，対象を限定しないで一括大量に収集する「バルクデータ」の重要性が高まっている．他方，2013 年 6 月にエドワード・スノーデンが秘密裡に行われていた NSA のシギント活動を暴露したことは，人々のプライバシー侵害の懸念を増大させ，同活動の法的な見直しにつながった．

本稿は，サイバーセキュリティ対策として，バルクデータの収集と分析が重要であることは認識しつつも，それを「通信の秘密」などの自由の保障とどう両立させれば良いか，について検討するものである．まずスノーデンの暴露によって，米国内でどのような法的見直しが行われたのかを紹介し，併せて EU-米国間でのプライバシー・シールド合意に至る経過を辿る．そしてバルクデータに関する扱いが，この法的見直しのなかでのどう見直されたかを考察する．その後，パケット解析やログの保存に関する法的解釈を確認した後で，バルクデータ収集・保存に関する法的問題を検討する．

## 1 はじめに

俗称イスラム国の登場などによって，事前にマークされていない犯人によるテロが頻発するようになったため，シギント活動においても，対象を限定して収集する「特定データ」ではなく，対象を限定しないで一括大量に収集する「バルクデータ」の重要性が高まっている．エドワード・スノーデン（Edward Snowden）が暴露した NSA(National Security Agency：国家安全保障庁)のシギント活動は，まさにそのような要請に応えるものであったが，余りに膨大な情報が秘密裡に収集されていたことは，人々のプライバシー侵害の懸念を増大させ，同活動の法的見直しにつながった．

スノーデンの暴露に対する最初の法的な見直しとして，2014 年 1 月 17 日にオバマ大統領は，PPD-28 号を発出した．その当日国務省で行われたオバマ大統領の演説では，インテリジェンス[1]活動とその一部であるシギント[2]（SIGINT：Signals Intelligence）活動の

*情報セキュリティ研究科 教授

†セキュアシステム研究所客員研究員

1 インテジェンスとは，「政策決定者が国家安全保障上の問題に関して判断を行うために政策決定者に提供される，情報から分析・加工された知識のプロダクト，あるいはそうしたプロダクトを生産するプロセス」のことを言う．出典：小林良樹[2014]

基本的な課題に関して，以下のような考えが述べられている．

1) 米国の歴史を通して，インテリジェンスは国家の安全と我々の自由を守るのに役立ってきた．さらにインテリジェンスは，9.11 以降突然従来以上の役割を果たすことが必要になった．
2) 現実の新たな脅威への対処において，政府の行き過ぎのリスクや核心的な自由の一部を失う可能性を，指摘されることが多くなった．
3) ICT 技術の進歩によって，差し迫った脅威に対処するために大量のバルクデータ[3]を収集できるようになったが，そのような収集と保存は濫用の危険も生み出している．
4) インテリジェンス活動は，秘密なしには成り立たない．それだけに公での議論が少なく，政府の行き過ぎの危険は大きくなる．技術が法よりも進歩が速い場合は，とりわけ大きくなる．このため自由・プライバシーと国家安全保障・人々の安全のバランスを，どう取るかの議論が必要である．
5) 国家権力の特性を考えると，指導者が「我々を信頼してほしい．収集したデータを濫用したりしません．」，というだけでは十分ではない．何故ならこの信頼は，歴史上数多く破られているからである．我々の政府システムは，我々の自由は権力者の良き意図（good intention）に頼ることはできないことを前提としている．我々の自由は，権力者を制約する法律を頼りにしている．

このオバマ大統領の演説は，人々の自由やプライバシーを守るのは，権力者の良き意図ではなく，法の支配(rule of law)[4]によるべきであって，安全と自由の両立を図るためには，適切な法制度が必要であることを指摘したものと考えられる．

また国家を成立させる 3 要素（主権，領土，国民）が失われると，プライバシー権の根拠とされる憲法 13 条などの基本的人権の規定を実現する基礎が失われることになるので，国家安全保障は国家存続に必要である．ところが国家安全保障のための法制度が，基本

---

『インテリジェンスの基礎理論［第二版]』立花書房

[2] シギントとは，「信号（data transmission）から収集される素材情報（中略）に基づくインテリジェンス」と定義される．シギントは，電子的な通信の傍受，加工，分析」を行う「コミント(COMINT：Communications Intelligence)」，と，レーダー等のから発せられる電磁波等を収集する「通信ではない信号の収集，分析」を行う「ELINT：Electronic Intelligence)」に大別される．この分類に従えば，本稿のシギントは COMINT である．
出典：小林前掲注 1 文献 p94

[3] PPD-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．

[4] 「法の支配」は民主主義国の普遍的価値の一つであるが，「人権の保障や民主主義の実現など，あるべき政治体制が備えるべき徳目のすべてを意味する理念として用いられる」という意味で使う場合には，「およそ政治体制について善いことはすべて法の支配に含まれること」になる．一方法哲学者や政治哲学者は，標準的には「人が法に従うことが可能であるために，法が満たしているべき条件」として，「法の公開性，明確性，一般性，安定性，無矛盾性，不遡及性，実行可能性」が法の支配の要請ということになる．出典：長谷部恭男[2011]『法とは何か』河出ブックス p148~156

的人権を侵害するとすれば，国家の必要性と正当性の基礎が失われる．

但し国家安全保障の目的[5]には，「国民の生命と財産を守る」ことも含まれていて，自由・プライシーと国家安全保障は重なりあっている部分もあるので，単純な２分法ではない．このような問題意識に基づいて，インテジェンス活動ないしシギント活動の法制度を検討する必要がある．

本稿でもこの観点から，シギント[6]活動の必要性が強まるなかで，国家と人々の安全に役立つシギント活動と自由・プライバシーを両立させるために，スノーデンの暴露を契機としてどのような法的見直しが行われたのか，その見直しのなかでバルクデータがどのように扱われているかを考察する．

日本におけるサイバー空間の安全を確保する法制度と，「通信の秘密」やプライバシーの権利との接点もしくは最適点を探るために，シギント活動で注目されているバルクデータを切り口に，その法的課題を探ることが本稿の目的である．

# 2 米英におけるシギント活動

## 2.1 2001 年 9 月 11 日同時多発テロの前後の法的規定

### 2.1.1 米国における同時多発テロ以前の法的規定

米国では国家安全保障の必要性から，インテリジェンス活動が認められており，この法的根拠は，大統領が国家安全保障に関して有する憲法上の権限であるとされている．中でもインテリジェンス活動は，国家安全保障のために行われるもので，信号情報に関するインテリジェンスであるシギント活動は，ネットワーク社会と呼ばれる現在その重要性が増大している．

シギント活動は，レーガン政権の初年度 1981 年に制定された大統領命令（Executive Order）12333 号に従って行われており，1952 年に設立された NSA が主としてその任に当たっている．

ところが1970 年代に入ってから，インテリジェンス活動の行き過ぎが問題になって，議会のいくつかの委員会で検証が行われ，1976 年 4 月にはチャーチ委員会の最終報告書が公表された[7].そこでの基本的検討課題は，「1. はじめに」で述べたことと同じく，国家安全保障上不

---

[5] 国家安全保障は，「自国の領土，独立，および国民の生命，財産を守る」ことであり，「冷戦時代には外敵による軍事的侵略から，軍事力によって守る」という意味合いが強かったが，現在では幅広い要素が含まれるとの考え方が多くなっている．この考え方の変化に対応して，インテジェンス活動の課題も，軍事的脅威の分析・評価から，国際テロ，国際組織犯罪やサイバーセキュリティなどまで広がっている．出典：小林前掲注 1 文献 p9~10.

[6] インテリジェンス活動は，国家安全保障の目的で行われるものである．従ってインテリジェンス活動の一部であるシギント活動も，国家安全保障のために行われるものである．出典：小林前掲注 1 文献 p94．この定義によれば犯罪捜査のために通信傍受は活動内容としては,COMINT 活動ではあるが，目的が異なるのでシギント活動に入らないことになる．.

[7] チャーチ委員会とその後の 1978 年の FISA 成立までの経過については，スノーデンの暴露の課題を検討するためにオバマ大統領が 2013 年 8 月に設置した検討グループが，同年 12 月に公表した以下の文献を参照．“Liberty and Security In a Changing World” Report and Recommendations of The President’s Review Group on Intelligence and

可欠なインテリジェンス活動と，その活動が侵害する恐れがある人々のプライバシーや自由との折り合いを，どうようにつけていくかであった.

これらの委員会での提言を実行するために，1978 年に FISA（Foreign Intelligence Surveillance Act：外国諜報監視法：1978 年成立, 1998 年改正[8]）が制定された. 中心的な課題は，外国諜報目的の電子的監視（electronic surveillance）の合法性であった.

1928 年の Olmstead 事件では，犯罪捜査における令状なしの通信傍受が合法とされたが，1967 年の Kats 事件は，「通信傍受（wiretapping）」は修正 4 条の保障する「プライバシーの合理的期待」に反するので令状が必要とされた. この犯罪捜査に関する判決の考え方が，国家安全保障のためのインテリジェンス活動にも適用されるかが議論された.

一般的には，大統領は国家安全保障に関する幅広い憲法上の権限を有していて，外国諜報監視を行うことも含まれている. このため修正 4 条の適用はないとの考え方であった. しかしながら FISA ではこの考え方を取らなかった. FISA では米国内での電子的監視を行うためには，行政権限だけではなく，権力分立の観点から裁判所の令状を要すると規定し，その手続きを行うために FISC（Foreign Intelligence Surveillance Court：外国諜報監視裁判所）を設立した. 一方で FISA は国外の活動に対しては適用外とした.

### 2.1.2 米国における同時多発テロ発生後の法的規定の見直し

2001 年 9 月 11 日の同時多発テロの発生を契機に，テロ対策を強化するための新たな法令の制定や既存法令の改正が行われた. 2001 年 10 月に成立した米国愛国者法（USA PATRIOT Act）215 条では，国際テロや秘密諜報活動（clandestine intelligence activities）への対策として，FISC の承認を受け，各種の業務記録を入手できることを定めている[9]. また大統領命令 12333 号が, 2003 年, 2004 年, 2008 年に改正されている.

このような法的見直しのなかにあって，NSA などのインテリジェンス機関の実際の活動の中には，人権保障の視点から法的に認められていないか，法的規定があいまいではないかとの批判や疑義が投げかけられていた.

これらの状況のなかで，「米国人に対する監視活動を厳格に規制する一方，外国人については，米国人の場合より監視活動の要件を緩和することで，テロ対策の実効性を確保すると見られる」[10]FISA 改正法が 2008 年に成立した. 1978 年の FISA が大統領のインテリジェンス活動の権限を制限する立法であったのに対して，2008 年改正法はインテリジェンス活動に対する民間事業者の協力義務と協力していることに関する守秘義務を規定しており，シギント活動を強化する内容も含んでいるとの指摘もある[11].

この改正法の規定によって，「外国の諜報情報だと合理的に信じられる場合であれば，FISC の許可を得た上で，1 年間通信傍受できることとなった.」，加えて「法律上，実質的な対

---

Communications Technologies, 12 December 2013.

[8] この改正によって，捜査目的のペンレジスターやトラップ・アンド・トレースの使用が認められた.

出典：鈴木滋「米国自由法：米国における通信監視活動と人権への配慮」 外国の立法 267(2016.3)p8

[9] 出典：鈴木前掲注 8 文献 p8

[10] 出典：鈴木前掲注 8 文献 p8~9

[11] 出典：「米国国家安全保障庁の実態研究」警察政策学会資料 第 82 号, 2015 年 9 月 p18～19

象の特定が不要になっている」との指摘[12]があるが，シギント活動を強化する内容になっているといえる.

### 2.1.3 英国における法的規定

英国におけるインテリジェンス活動は明確な根拠法がなく行われていたが，1985年に通信傍受法（Interception of Communications Act 1985）が制定された．その後国家安全保障や犯罪捜査のために，通信傍受やコミュニケーション・データの取得に関して，通信傍受法の内容を改正するRIPA(Regulation of Investigatory Powers Act：調査権限規制法)が2000年に制定されている.

2001年9月の同時多発テロ発生後に，テロリズム防止に関する立法が何回かなされている[13].

2005年7月にはロンドンでも同時多発テロが発生した．これに対応して，2006年のテロリズム法ではRIPAが一部改正され，傍受令状の有効期限を3カ月から6カ月に延長するなどの権限強化が行われた[14].

法的な手続きに関しては，米国では司法手続きが原則になっているのに対して，英国では行政手続きだけで通信傍受等が行われているのが特徴的である．以上の2.1全体の経過をまとめたのが表1である.

.

表1： 9.11の前後の米英のシギントに関する法的規定

| | 米国 | 英国 |
|---|---|---|
| 9.11以前 | 大統領令12333号制定：1981年<br>FISA:1978年成立，1998年改正 | RIPA：2000年成立 |
| 9.11以降 | 愛国者法成立：2001年<br>大統領令12333号改正：2001年<br>FISA改正：2007年，2008年 | テロリズム法成立：2006年 |

## 2.2 エドワード・スノーデンのNSAの活動に関する暴露の影響

2013年6月にスノーデンが，NSAが秘密裏に行っていたプリズム（PRIZM）やアップストリーム（UPSTREAM）などのシギント活動によって，米国内外の市民の個人データが大量に収集されている現状を暴露したことで，NSAの活動が米国の法令で認められた活動なのか，法律に違反していないとしても憲法上許される行為なのかについて米国内外で多くの論議が行われた．現に，違憲訴訟も提起されている.

---

12 出典：大林啓吾[2015]『憲法とリスク』弘文堂 p186~187

13 以下の文献を参照．岡久慶「イギリスの2015年対テロリズム及び安全保障法」外国の立法265号（2015.9），
同「イギリスの2011年テロリズム防止及び調査措置法」外国の立法267号（2016.3）

14 以下の文献を参照．小谷賢「8 英米における情報機関の行政権限」大沢秀介監修『入門・安全と情報』

### 2.2.1 米国における法的見直し

(1) 大統領による検討チームの報告書公表とPPD-28号の発出

2013年6月のスノーデンの暴露の2か月後の8月に，オバマ大統領は5人の検討グループによって検討を開始した．この検討グループには，安全保障問題で著名なリチャード・クラーク（Richard A. Clarke）や憲法学者のキャス・サンスティーン（Cass R. Sunstein）が加わっている．

検討グループの最終報告書は，同年12月に公表された．この報告書では9.11以降拡大された法的規定が，個人の自由・プライバシーおよび民主的ガバナンスを不当に犠牲にしていると結論づけて，46の提言を行っている[15]．

上記の最終報告書を基礎にして，翌月の2014年1月17日に発出したのが，第1章で述べたPPD-28号である．なお後述するように，EU-米国間のプライバシー・シールドでも，米国における法的見直し内容について詳しく述べられている．PPD-28号4条には，この指令内容を反映した方針と手続き（policies and procedures）を1 年以内に定めることが規定されているが，2015年1月にNSAはこの規定に従った手順を定め公表している．

(2) 米国自由法（USA Freedom Act of 2015）

この法律成立の背景として，愛国者法が2015年5月末で効力を失うことで電話のメタデータ収集の根拠がなくなること，2015年5月に第2巡回連邦控訴裁判所が政府のメタデータ収集の違法性を認めた判決を下した，という2つの事情があった．

この状況の中で，最終的には期限切れ直後の6月2日に議会で可決され，大統領の署名を得て即日成立した「米国自由法」では，通信記録の提出命令やペンレジスターやトラップ・アンド・トレースを用いた通信監視活動の承認をFISCに請求する場合に，対象情報を特定しなければならないとの規定が設けられた．

これらの規定は，バルクデータの収集は行わないとする規定であるように考えられる．

(3) 司法救済法(Judiciary Redress Act of 2015)

法案は2015年3月に議会に提出され，10月に下院を通過，2016年2月に上院で修正可決された後に，下院でも可決されて成立した．この法律では，EU市民が個人情報の不法な開示に対して，米国プライバシー法の規定に基づいて米国政府を訴えることができることとした．

### 2.2.2 EU-米国間のプライバシー・シールドの発効までの経過

スノーデンのNSA活動の暴露の影響は米国だけにとどまらず拡大する様相をみせた．その一つとしてEU市民の個人データを米国に移転するために，EU-米国間の枠組みとして2000年にスタートしたセーフハーバーにも影響が及んだ．スノーデンの暴露によって，セーフハーバーが保障している保護レベルが，実際には十分に守られていないのではないかとの疑念が，EU側に生じたのである．

そこでまずEU内部において，セーフハーバーの見直しについて検討が行われた．この検

[15] 前掲注7文献p77

討結果が, 2013 年 11 月に EU 委員会が公表した「EU-米国間のデータ流通における信頼の再構築」である. そして 2014 年に入ってから EU-米国間での見直し交渉が始められたが, この交渉途中の 2015 年 10 月には, EU 司法裁判所でセーフハーバーが無効であるとの判決が下されたことで, セーフハーバー見直しは必須の状況になり, 交渉が加速された.

この間に米国では前 2.2.1 で述べたような法的見直しが行われたこともあって, 米国へ移転された EU 市民の個人データに対する保護水準は, EU の個人データの保護水準と同等なレベルにあると認定されたことで, 2016 年 2 月に政治的(大筋)合意がなされた.

この 2 月の政治的(大筋)合意以降, 個人情報保護を担当している 29 条委員会や欧州議会など EU 内部で最終的な調整が行われた. この最終調整の過程で追加されたのが, ① バルクデータ収集に関する追加的な明確化, ② オンブズパーソンの仕組みの強化などである. 以上の経過を経て, セーフハーバーに代わって新たにプライバシー・シールドが 2016 年 7 月に発効している.

プライバシー・シールドでは, 米国企業のデータの取扱いに関する強い義務, 米国政府への明確な安全管理措置と透明性の義務, 個人の権利の効果的な保護のために個人の権利が侵害されたと考える EU 市民が直接紛争解決する手段などが重層的に用意されている[16]. 以上の一連の経過をまとめたのが表 2 である.

表 2: プライバシー・シールド協定発効までの時系列(経過)

| EU 側の動向 | プライバシー・シールド協定 | 米国側の動向 |
|---|---|---|
| 2013 年 11 月:EU 委員会「EU-米国間のデータ流通における信頼の構築」公表 | | 2013 年 12 月:「変化する世界における自由とセキュリティ」公表 |
| | 2014 年見直し交渉開始 | 2014 年 1 月:PPD-28 号発出<br>2015 年 1 月:NSA:PPD-28 Section 4 Procedures 公表<br>2015 年 5 月:第 2 巡回連邦控訴裁判所の政府のシギント活動への違法判決 |
| 2015 年 10 月:EU 司法裁判所の「セーフハーバー」無効判決 | | 2015 年 6 月: USA FREEDOM Act 成立 |
| EU 内部の調整 | 2016 年 2 月政治的合意<br><br>2016 年 7 月 12 日発効<br>EU 委員会十分性決定<br>ANNEX Ⅰ ～Ⅶ | 2016 年 2 月:司法救済法成立 |

[16] プライバシー・シールドの大まかな概要は, 以下の文献を参照. "EU-U.S. Privacy Shield FAQ: Fact Sheet, Brussels, 12 July 2016

| | | |
|---|---|---|
| | 2016 年 8 月　米国企業の登録開始 | |

### 2.2.3　英国の法的対応

イギリスのインテリジェンス機関は，長年米国のインテリジェンス機関と緊密な協力関係のもとで活動してきた．スノーデンの暴露は，英国のガーディアン紙などによるインタビューが元になっており，また同紙が機密とされていた暴露情報の記事を多く掲載したことや，英国のシギント活動の内容も報じられたことで，スノーデンの暴露は英国のインテリジェンス機関にも大きな影響を及ぼした．

暴露直後に主要インテリジェンス機関である MI5（保安部），MI6（秘密情報部，SIS），シギントを担当する GCHQ（Government Communications Headquarters：政府通信本部）のトップが議会で証言したり，米国インテリジェンス機関との緊急協議などの対応が行われた．もっとも，英国では伝統的にインテリジェンス活動の必要性に対する理解や支持があるとされている．

スノーデンの暴露の翌年 2014 年 4 月に，EU の欧州司法裁判所がデータ保全指令を無効とする判決を下した．これに対する法的対応として，2014 年 7 月に DRIPA（Data Retention and Investigatory Powers Act 2014：データ保全及び調査権限法）が成立した．

この法律では，通信データの保全規定の整備とともに，RIPA 第 1 章が規定する「通信傍受令状などが英国国外の電気通信役務提供者に対しても有効であることを明記している」[17]．なお DRIPA には 2016 年 12 月末に失効するサンセット条項がついていて，その時期までに新たな立法が必要になっている．

この事態を受けて，スノーデンの暴露以降のインテリジェンス活動が，過度な人権侵害につながらないように RIPA の見直し検討が行われて，2015 年 11 月に調査権限法案（Investigatory Powers Bill）の政府案が公表された．同法案は法執行機関やセキュリティやインテリジェンス機関による調査権限の行使と監督するための新たな枠組みを作るものである．

同法案は 2016 年 3 月に下院に提案され，下院の審議を経て，EU 離脱に関する国民投票が行われた 6 月 23 日に先立つ 6 月 7 日に，賛成 444 票対反対 69 票の圧倒的多数で修正可決され，上院に送付された．本論文の執筆時現在（10 月 2 日）では，上院では 9 月 12 日までに委員会段階を終了した．以後 Report Stage, Third Stage を経て採決が行われる．

## 2.3　米英のインテリジェンス機関

### 2.3.1　米国のインテリジェンス機関

インテリジェンス機関の統合を目指して 2004 年の法律で，新規に創設された DNI

[17] 出典：今岡直子「イギリスにおけるデータ保全及び調査権限法の制定：EU データ保全指令の無効判決を踏まえて」 外国の立法 264（2015.6）p2

（Director of National Intelligence：国家情報長官）制度をはじめとして，国防省所属のNSAなどの８つの軍事系インテリジェンス機関，７つの各省庁所属のインテリジェンス機関および独立のインテリジェンス機関（CIA：Central Intelligence Agency：中央情報局）の合計 17 のインテリジェンス機関がある．

またインテリジェンス機関全体で 2013 年会計年度の予算額は，676 億ドルと巨額である．なお人員は明確なものは公表されていないが，総数で約 20 万人以上との推測もある[18]．

### 2.3.2 英国のインテリジェンス機関

英国内と大英帝国の調査活動を行う MI5 と海外での調査活動を行う MI6 は，1909 年に設置されているが，1989 年になって MI5 の根拠法である Security Service Act 1989 が制定され，MI5 の存在が公式に認められるようになった．また 1994 年に MI6 と GCHQ の根拠法である Intelligence Services Act が制定された．

なおプライバシーの保護規定には，データ保護法のほか，欧州評議会の制定した欧州人権条約や人権法（Human Rights Act 1998）がある．

### 2.3.3 UKUSA 協定

米英のシギント活動は，第 2 次世界大戦時から両者の緊密な連携のもとに行われているが，1946 年には UKUSA 協定の原型となる協定が米英間で締結され，その後カナダ，オーストラリア，ニュージーランドも加わった．これらの 5 か国は five eyes とも呼ばれ，連携してシギント活動を行っている[19]．

## 3 シギント活動に関する法制度見直しの注目点：バルクデータ

前 2 章の法的見直しで焦点となったのは，インテリジェンス機関による情報の収集・分析・保存が，法令で規定されている範囲や限度を超えているのではないか，また市民のプライバシーを侵害しているのではないかとの疑念であった．とりわけ人々のプライバシーや自由を侵害する可能性の高い，バルクデータの収集・分析・保存についての規定見直しに関心が集まっている．そこで米国における法的見直し，EU-米国間のプライバシー・シールドおよび英国の法制度見直しに関して，バルクデータがどのように規定されているのかをみてみよう．

---

[18] 出典：小林前掲注 1 文献 p60～67

[19] インテリジェンスの歴史的経過については，以下の文献に詳細に説明されている．小谷賢[2015]『インテリジェンスの世界史』岩波書店

### 3.1 スノーデンが暴露した NSA のシギント活動[20]

スノーデンが暴露した NSA のシギント活動は多岐にわたり，解明されていないものも多いが，そのなかで多くの注目を浴びたのは，「プリズム・プログラム」と，「電話のメタデータ収集」，「アップストリーム・プログラム」の 3 つである.

そこで以下では，特定者を対象とする「特定データ収集」と，特定者を対象とせずに一括大量の「バルクデータ収集」の二つに分けてその対象と手法を分析する.

#### 3.1.1 プリズム・プログラム

このプログラムは，インターネットインフラやインターネット接続サービスを提供している通信事業者ではなく，そのインフラを利用してフリーメールや SNS サービスなどを提供しているOTT（Over the Top）と呼ばれるマイクロソフト，ヤフー，グーグル，フェイスブック，アップルなど 9 社の協力を得て，9 社が記録保存しているデータまたは通信中のリアルタイムデータを取得するものである.

収集対象は，通信内容・コンテンツ情報と通信に伴って得られるメタデータ[21]の両方である.収集方法としては，各社のデータセンタ内に FBI がデータ収集装置を設置して行っている.

情報取得は e メールアドレスや IP アドレスによって，NSA 職員が直接データを取得できるが，対象が米国人である場合には取得できない仕組みがあるようである．またリアルタイム監視の対象者は，ワシントンポスト紙の報道では約 12 万件である.

プリズム・プログラムで収集されるデータは，対象が幅広いものの，e メールアドレスや IP アドレスを指定したり，オンライン監視対象が事前に登録されていたりしており，バルクデータ収集ではなく，特定データ収集ではないかと考えられる.

このプリズム・プログラムの法的根拠は，FISA702 条である．この 702 条では，米国人に関する情報を極力収集しないように，標的決定手順（702 条（d））や最小化手順（101 条（h））が定められているが，かなりの米国人に関する情報が付随的に取得されていたとみられている.

---

[20] この項については以下の文献を参照．前掲注 11 文献「米国国家安全保安庁の実態調査」．大林前掲注 12 文献． 石井夏生利[2014]「第 5 章 米国の国家安全と監視強化」『個人情報保護法の現在と将来』勁草書房．宮下紘[2015]「Ⅲ 安全 vs プライバシー」『プライバシーの復権』中央大学出版部．グレン・グリーンウオルド[2014]『暴露』新潮社．ルーク・ハーディング[2014]『スノーデンファイル』日経 BP 社．デイヴィッド・ライアン[2016]『スノーデン・ショック』岩波書店

[21] このメタデータは，日本の通信の秘密法制では「通信の構成要素」，英国の法制では「コミュニケーション・データ」と呼ばれる通信内容以外の情報を意味する．インターネットのパケットでは，ヘッダーにある情報である.
プリズム・プログラムは，「外国の標的が利用する電子メール，チャット（動画，音声），ビデオ，写真，蓄積データ，VoIP（Voice over Internet Protocol），ファイル交換，ビデオ会議，ログインターネットなどの標的の活動に関する通知，ソーシャルネットワーキングの詳細などを NSA と連邦捜査局（Federal Bureau of Investigation：FBI）が収集する計画である.」出典：石井前掲注 18 文献 p239.

### 3.1.2 愛国者法 215 条を根拠に行われている電話のメタデータ収集

米国内で米国人も対象にする電話のメタデータを，包括的に収集する活動が行われていた．この収集活動は同時多発テロ直後から，大統領命令によって密かに行われていたが，AT&T，ベライゾンなど電話会社３社の任意の協力を得てこの活動を行っていることが，2005 年 12 月にニューヨークタイムズ紙の暴露報道で明るみにでた．

電話のメタデータ収集が開始された経過は，以下の通りである．「（9.11 の同時多発テロ後に）NSA 長官はブッシュ大統領からテロ対策のための情報収集活動の強化を命ぜられたが，NSA 長官はその対策の一つとして通信メタデータの収集を提案した．」これは通信メタデータの分析によって，「未知のテロリストを発見しようとするものである」「（この電話のメタデータ収集によって）世界の国際電話の 27%が米国の民間事業者の協力で，捕捉できたということになった．」[22]

暴露報道がなされたことで，電話会社３社の自発的協力が得にくくなったために，メタデータ収集を続けるべく，愛国者法 215 条のビジネス記録として提出命令が出せるとの解釈が打ち出された．メタデータは通信事業者が自らの業務上の必要性に基づいて収集した業務記録(business record)であるため，第三者法理(Third Party Doctrine)によって，「合理的なプライバシーの期待」が生ぜず，従ってその収集に憲法修正４条が規定する不合理な捜索と押収には該当しないとの解釈が取られたのである[23]．

ところが連邦第二巡回控訴裁判所は，2015 年 5 月にこの収集方法が違法であるとの判決を下した．加えて愛国者法は 2015 年 5 月末に失効することで，この愛国者法 215 条を根拠とする解釈を取ったとしても，根拠法が失われることになった．

それまでの膨大で包括的な電話のメタデータ収集に対する批判にも応える形で，議会が愛国者法 215 条の失効直後の 6 月 2 日に成立させたのが「2015 年米国自由法」である．「法律のポイントは，FISA の基本的枠組みを維持しつつ，① 大量収集プログラムを停止し，② 情報収集の範囲と情報保存期間を限定し，対象者への影響を最小限にとどめ，③ 通信監視活動及び FISC の透明性を高めることである[24]．」

この 2015 年米国自由法によって，従来行っていた電話のメタデータの包括的な「バルクデータ収集」が禁止され，収集対象者を限定する「特定データ収集」に変わったと考えられる．

### 3.1.3 民間事業者の協力を得て行われているインターネットの基幹回線の主要ポイントにおける膨大なデータ収集プログラムである「アップストリーム・プログラム」

NSA はアップストリーム・プログラムなどによって，インターネットの基幹回線にアクセスし

---

[22]「 」内の記述の出典：前掲注 11 文献「米国国家安全保安庁の実態調査」p66～68

[23] 米国における第三者法理については，以下の文献を参照．Richard M. Thompson Ⅱ[2014] “The Fourth Amendment Third-Party Doctrine”, Congressional Research Service．またこの第三者法理の妥当性が問われていることについては，以下の文献を参照．湯淺懇道「位置情報の法的性質―United States v. Jones 判決を手がかりに―」情報セキュリティ総合科学 第 4 号 2012 年 11 月号

[24] 出典：前掲注 8 文献 p13

て，大量のデータを一括収集している．この収集されたデータはバルクデータであり，一定期間（通信内容・コンテンツは 3 日間，メタデータは 30 日）保存され，抽出された必要情報は別のデータベースに長期間保存される[25]．アップストリーム・プログラムの法的根拠は FISA702 条である．(3.3.2 参照)

同様のプログラムが，英国の GCHQ によって行われていて「テンポラ・プログラム」と呼ばれているが，NSA による収集プログラムよりも，はるかに大量のバルクデータを収集している．

なお外国通信衛星の傍受なども，アップストリーム・プログラムとは異なるプログラムであるが，バルクデータ収集である．

以上の 3 つのプログラムにおける収集対象を比較したのが表 3 である．

表 3: スノーデンが暴露した 3 つのプログラムの収集対象の比較

| | 通信内容<br>コンテンツ | メタデータ | 特定データ | バルクデータ |
|---|---|---|---|---|
| プリズム・プログラム | ○ | ○ | ○ | |
| 電話のメタデータ収集 | | ○ | | ○ |
| アップストリーム・プログラム | ○ | ○ | | ○ |

## 3.2 米国における法的見直しにおけるバルクデータ

PPD-28 号では，以下の内容が定められている．

1) 新しいもしくは顕在化しつつある脅威はネットワークに潜んでいるので，それを見つけ出すにはバルクデータ収集が必要であるが，外国諜報活動の対象者以外の人々の情報も集めてしまうことになる．

2) バルクデータを収集する場合であっても，その利用は以下の 6 項目の国家安全保障目的に限定する．(2 条) ① 外国勢力等によるエスピオナージなどの脅威，② テロの脅威，③ 大量破壊兵器の開発，保有，拡散および利用，④ サイバーセキュリティ，⑤ 米軍や同盟軍または米国人や同盟国人への脅威，⑥ 国境を超える犯罪の脅威

3) シギント活動で収集された個人情報への安全管理措置を講ずる．(4 条) 例：方針と手続きに関する事項（情報共有・配布・保存の最小化，データセキュリティとアクセス，データの正確性（quality），監督(oversight).

また 2015 年米国自由法では，通信記録の提出命令やペンレジスターやトラップ・アンド・トレースを用いた通信監視活動の承認を FISC に請求する場合に，対象情報を特定しなければならないとの規定が設けられた[26]．これらの規定は，バルクデータの収集を行わないとする規定であるように考えられる．

---

[25] 出典：前掲注 11 文献 x i x

[26] 通信記録の提出は 501 条，ペンレジスター等の場合は 201 条に規定されている．出典：前掲注 7 文献 p14

## 3.3 EU-米国間のプライバシー・シールドにおけるバルクデータ

### 3.3.1 プライバシー・シールドの構成

2016 年 7 月 12 日に発効したプライバシー・シールドは，本文 “Commission Implementing Decision of 12.7.2016：(中略)adequacy of the protection provided by the EU-U.S. Privacy Shield” と ANNEX Ⅰ～Ⅶから構成されている．この本文において EU 委員会は，プライバシー・シールドが EU の個人データ保護法と同等の保護水準にあると認定した．

本文は 44 ページあるが，そのうち「1. はじめに（Introduction）」では交渉経過が 3 ページ,「2. プライバシー・シールド（The “EU-U.S. Privacy Shield）」では概要が 12 ページにわたり記述されている．「3. プライバシー・シールドのもとで米国に移転された EU 市民の個人データへの米国の公権力によるアクセスと利用(Access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities)」が 22 ページと，残りのほとんどのページを占めていることから分かるように，スノーデンの暴露によって明らかになった米国政府のシギント活動の実態が，セーフハーバー見直し交渉の主たる契機になっていることを伺わせる文書になっている．

### 3.3.2 プライバシー・シールドの内容

「3.1.1 制限（Limitations）」に，以下のようなバルクデータに関する記述が多くみられる．なお各項目の後の番号は，項目番号である．

1) 米国憲法では，国家安全保障の確保は大統領の権限である．これには外国諜報も含まれる．議会は制限を課すことができるが，その範囲内で大統領はインテリジェンス機関の活動の指揮を執ることができる．現在の中心的な法的手立ては，大統領令（Executive Order）12333 号と PPD（Presidential Policy Directive：大統領政策指令）28 号である．[68]

2) PPD-28 号はシギント活動にいくつもの制限を課しており，米国のインテリジェンス活動を拘束するものである．PPD-28 号は EU 市民を含む非米国人にとって特に重要である．[69]

3) シギント活動は外国諜報または防諜目的のためにだけ行われるもので，収集は識別子（discriminants, e.g. specific facilities, selection terms and identifiers）を利用して，特定の外国諜報対象に向けて行われると，ODNI（Office of Director of National Intelligence：国家情報長官室）は説明している．[70]

4) 特定データ収集は，バルクデータ収集よりも優先するのが一般原則である．また ODNI は，バルクデータ収集は大量（mass）でも無差別(indiscriminate)でもなく，例外が一般化することはないことを保障している．[71]

5) PPD-28 号ではバルクデータ収集を行う必要がある場合には，特定データ収集を可能にするような代替策を優先するよう規定していて，バルクデータ収集は対象者の e－mail アドレスや電話番号のような識別子が利用できない場合にのみ行われる．[72]

6) 特定データを収集する際に一致語（identifiers）が利用できない場合に，可能な限り収集範囲を狭めるようにすると説明されている．米国のシギント活動はインターネットを流

れている通信のわずかな部分しか扱っていない．また無関係な情報収集を最小化するために，できるだけ詳細にデータ収集範囲を絞るように，フィルターなどを利用していると説明されている. [73]

7) バルクデータ収集を必要とする場合であっても，PPD-28 号ではその利用は特定の 6 項目の国家安全保障目的に限定されている. [74] (3.2.2 参照)

8) これらの制限はプライバシー・シールドの下で移転された個人データに適合的である．特に個人データの収集が米国外で行われる場合に適合的である．これには EU から米国への大西洋横断ケーブルでの伝送中の個人データを含んでいる. [75]

9) 法律用語を用いてはいないものの，これらの原則は必要性と比例性の原則の本質を踏まえている．特定データ収集は明らかに優先されており，バルクデータ収集は特定データ収集ができない例外的な場合に制限されている. [76]

10) 米国自由法は，FISA402 条（ペンレジスターとトラップ・アンド・トレース権限），FISA501 条（旧愛国者法 215 条）および NSL(National Security Letter：国家安全保障令状)を根拠とするバルクデータ収集を禁止しており，代わって特定の選択語(selection terms)を利用することを要求している. [79]

11) FISA702 条は，プリズム・プログラムとアップストリーム・プログラムの根拠になっているが，対象の e－mail アドレスとか電話番号のような特定の通信設備を特定する個別の選択語を利用して，対象を絞った形で探索が行われている．FISA702 条にはサンセット条項があって 2017 年に期限が来るが，そのときに EU 委員会は EU 市民が利用できる安全管理措置の再評価を行う予定である. [81]

12) 米国のインテリジェンス機関は，一般のヨーロッパ市民を含む誰に対しても，無差別な監視を行っていないと米国政府は EU 委員会に保障している．米国内で収集されている個人データに関しては，インターネット上を流通している全体のデータと比べれば，相対的に少数しか対象になっていないことは，NSL や FISA によるアクセス要求に関する経験的な証拠によって支持されている. [82]

13) 正当なプライバシーや市民的自由を守ることと，シギント活動の実践的必要性とのバランスを取ることが必要であることを，米国政府は説明している. [85]

プライバシー・シールドではこの他, need to know 原則[27]によって，権限のある者からのアクセスを限定すること，個人情報を適切な保護の下で処理，蓄積することなどデータセキュリティに関する事項，データの配布と保存を最小化するような安全管理措置を取ること，保存期間は例外を除き最長 5 年に制限することなども規定されている.

### 3.4 英国の調査権限法案（Investigatory Powers Bill）におけるバルクデータ

法案の詳細な分析はこれからであるが，英国の考え方は以下のようなものと推定される．技術的な変化によってセキュリティとインテリジェンス機関が直面している課題は変化して

[27] Need to Know 原則とは，「軍事情報など機密性の高い情報を扱う部門では『Need to Know の原則』が強調される．これは『(仮にアクセス権があっても) 現在の職務に必要な情報しかアクセスしないし，させない原則』をいう．」 出典：林紘一郎・田川義博・淺井達雄[2011]『セキュリティ経営』勁草書房 p69

いる. テロリストや犯罪者は現代の通信ネットワークを, 計画, 調整, 攻撃するために利用している. インターネットや暗号の発展によって, 伝統的な対象を特定したインテリジェンスのアプローチでは, これらの課題に応えることが困難になってきている.

バルク権限は過去 10 年間セキュリティとインテリジェンス機関にとって不可欠となっており, 将来的にはますます重要になっている. バルクデータの取得と利用(大きな規模で取得され, 特別な制約に服して利用される情報)は, セキュリティとインテリジェンス機関にとって, 他の手段では得られないユニークなインテリジェンスを与えてくれる.

これらの機関はもっとも重要な国家安全保障の課題を克服するために, 現代の企業がデータ分析にますます依存している手法と同じ手法を利用しているが, 厳格な安全管理措置と強力な監督に服している.

議会で審議中の調査権限法案(Investigatory Powers Bill)では, 犯罪捜査や国家安全保障のために, 7 種類のシギント情報の収集権限を規定している.

通信傍受(interception of communications), コミュニケーション・データ取得(authorization of obtaining of communications data), 機器への介入(equipment interference)の 3 つは, 対象を限定した特定データ取得のための権限である.

これに対してバルクデータ収集に関しては, 以下の 4 つの令状権限が規定されている. すなわち, バルク通信傍受令状(bulk interception warrant), バルク令状(bulk warrant ), 機器への介入令状(bulk equipment interference warrant), バルク個人データセット令状(bulk personal datasets warrant)である.

これらのバルク権限は従来から 既存の他の法律で認められていたが, 今回の調査権限法に集約して規定するものである.

・バルク通信傍受:RIPA2000
・バルク機器介入:Intelligence Service Act1994
・バルクパーソナルデータ:Intelligence Service Act1994 and Security Act1989
・バルクコミュニケーションデータ:Telecommunications Act1984

## 3.5 バルクデータに関する論点

### 3.5.1 スノーデンの暴露以降の米国における法的見直し

バルクデータ収集は広く大量のデータを収集するので, 特定データ収集よりも自由やプライバシー侵害のリスクは大きくなる. そこでこれまで述べたように, スノーデンの暴露以降に新たに成立した PPD-28 号や米国自由法では, 以下のような見直しが行われた.

1) 特定データ収集を原則として, バルクデータ取集を例外とする(3.3.2 参照), もしくはバルクデータの収集を止める(3.1.2 参照).

2) 外国諜報のためのシギント活動では, 識別子(discriminants)を利用して, 収集対象データを限定する (3.3.2 参照).

3) バルクデータ収集を行う場合でも, その利用は 6 項目の国家安全保障目的に限定する(3.2)参照).

### 3.5.2 考察

(1) プライバシー・シールドの下で移転された EU 市民の個人データは，プライバシー・シールドで守られたとしても，PPD-28 号や米国自由法を根拠にした特定データやバルクデータ収集が，EU 市民を含め他の外国人等をプライバシー・シールドが適用されない領域，手法でも行われているとすれば，EU 市民のプライバシー全体がプライバシー・シールドで保護対象になっているといえるのだろうか．

(2) PPD-28 号などの米国法の規定とプライバシー・シールドの記述が，整合しないところがあるように考えられる．プライバシー・シールドでは indiscriminate なバルクデータ収集は行わない，またバルクデータは mass でも indiscriminate でもないとしている(3.3 4)参照)．この記述が正確であるとすれば，PPD-28 号 2 条注 5 に規定されているバルクデータの定義が変わっているようにも考えられる．

(3) さらに収集しているデータ量は，インターネット上を流通しているトラフィックのうちのわずかな割合にしかなっていない（only a fraction of the communications traversing the internet）（3.3 6）参照）としているが，スノーデンの暴露した内容とは異なる印象を受ける．

プリズム・プログラムでは，グローバルでの大きなシェアを占める米国 OTT 企業が協力しているが，それらの企業が米国内に多くのデータセンタを置いているので，スノーデンのいうように大量のシギント情報を NSA に提供していたと考えられる．またアップストリームやテンポラ・プログラムで，インターネットの基幹回線から大量の情報を収集・分析できるのも，米英を経由する光ファイバーケーブルが多いからであると考えられる．

しかし一方で，スノーデンの暴露以降の情報収集方法の見直しによって，バルクデータ収集が減少して特定データ収集が増えたとすれば，このわずかな割合という表現に多少の真実性があることも考えられる．

(4) 収集したバルクデータから分析手法を活用して，特定データを抽出しているのが，通常の手順である．したがってバルクデータ収集を行ったとしても，バルクデータ取集自体が目的ではなく，シギント情報として有用な特定データが抽出された後に廃棄されれば，シギント情報収集・分析の対象外である人々の自由やプライバシーが侵害されるリスクはそれほど大きくないのではないかと考えられる．

仮にバルクデータ収集であったとしても，収集自体は機械的・自動的に行われている．このため人間の意思を持たない機械的・自動的なデータ収集が行われても，プライバシーが侵害されたことにはならない，とのリチャード・ポズナー（Ricard A. Postner）の指摘や，プライバシー権が問題になるのは公開の場面であって収集の段階では問題にならない，とのスタンツ（William J. Stuntz）の指摘[28]がある．

(5) しかしながら，バルクデータが一定期間保存されている場合に，情報の安全管理措置が不十分で，外部からの攻撃や内部者の情報持ち出しによって，その情報が漏えいすると，シギント情報の対象外の人々の自由やプライバシーが，侵害されるリスクが高くなると考えられる．この観点からは，内部において need to know 原則を実際にどう適用するかも重要になると考えられる．

---

[28] 出典：大林前掲注 12 文献 p199

(6) また保存されているバルクデータが，他の目的に利用されるとすれば，人々の自由やプライバシーが，侵害されるリスクが高くなると考えられる. PPD-28 号 2 条では，収集されたバルクデータを政権に対する反対者への抑圧や人種・宗教による不利益扱いをする目的では利用しないことを明確にしている.
(7) プリズム・プログラムでは, ISP ではなく, OTT 事業者がデータを提供していたことが明らかになったが，OTT 事業者が大量かつセンシティブな情報を保有しており，シギント活動において OTT 事業者の役割にも注目すべきであると考えられる.

# 4 ISP 等[29]のパケット解析・ログの保存とその法的解釈

これまで米国などのシギント活動におけるバルクデータや特定データ収集について述べてきたが，4 章以降は我が国のサイバーセキュリティに関して，バルクデータや特定データ収集の問題について考察する.

## 4.1 ISP 等のパケット解析・ログの保存[30]

### 4.1.1 ISP が自らのサービス提供のために行うパケット解析とログの保存・分析

ISP は自らのサービス提供のために，以下の目的などでパケット解析を行い，ログの保存・分析を行っている.

1) 正当な(接続)業務を行うための例:認証ログ(認証・認可・課金)
   ・認証(authentication):契約者のパケットかどうかの確認
   ・認可(authorization):当該サービスに接続してよいとの認可
   ・課金(accounting)
2) 安定的なサービスを提供するための例
   ・イベントログ:故障等の以上の検知，ログイン・ログアウト等の記録
   ・セキュリティログ:攻撃検知やポリシー違反発生時の記録

これらの例は，いずれも自らのサービスを円滑に提供するために必要なパケット解析であり，ログの保存である.

### 4.1.2 犯罪捜査などにおけるログの利用

通信履歴[31]は，事業者自らの業務上の必要性とは別に犯罪捜査のためにも利用される

---

29 ISP 以外にもパケット検査やログの保全を行っている事業者がいるので「等」としている. 例えば OTT(Over the Top)事業者も自らのマーケティングに利用するためにパケット検査やログの保管や分析を行っている. またブロードバンドサービスを提供している NTT 東西も故障時の故障個所の特定や苦情・問合せ対応のためにログの保管や分析を行っている.

30 4 章の記述については, NTT コムの小山覚氏に知見をいただいた. ここに謝意を表したい.

31 通信履歴に関する規定については,「電気通信事業における個人情報保護に関するガイドライン(平成 16 年 8 月 31 日総務省告示第 695 号, 最終改正 平成 27 年 6 月 24 日総務省告示第 216 号)」および「同ガイドラインの解説」23 条を参照.

ことがある. 刑事訴訟法 197 条では,「通信履歴の電磁的記録のうち必要なものを特定し, 30 日を超えない期間を定めて, これを消去しないよう, 書面で求めることができる(3 項)」,「特に必要があるときは, 30 日を超えない範囲内で延長することができる. ただし, 消去しないように求める期間は, 通じて 60 日を超えることができない.(4 項)」と規定されている.

この規定の前提は, これらの通信履歴については, 裁判官の発する令状によって通信履歴を差押えることができるとの(同法 218 条 1 項)規定である. 197 条の趣旨は, それ以前に通信記録が消去されることを防ぐことである.

### 4.1.3 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

電気通信事業に関しては, 個人情報保護法及び通信の秘密に係る電気通信事業法 4 条等の規定を遵守するほか,「このガイドラインに従って個人情報を適正に取り扱う(第 3 条 2 項)」ため, ガイドラインが解説とともに総務省告示として公表されている.

(1) ガイドライン 10 条の規定

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. 但し「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)).

(2) ガイドライン 23 条の規定

1 項において,「電気通信事業者は, 通信履歴(利用者が電気通信を利用した日時, 当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のものをいう. 以下同じ.)については, 課金, 料金請求, 苦情対応, 不正利用の防止その他の業務の遂行上必要な場合に限り, 記録することができる.」と規定されている.

この規定は 4.2 において後述するように, 通信履歴は「通信の秘密」の一部である通信の構成要素であって, 電気通信事業者といえども,「業務遂行上必要な場合に限り, 記録することができる」もので, 記録行為について制約を設けている規定と考えられる.

この規定はまた自己利用を想定しているので, 他人に提供することはごく例外的にしか認められていない. 2 項では,「裁判官の発布した令状に従う場合, 正当防衛又は緊急避難に該当する場合その他の違法性阻却事由がある場合」のみを 1 項の例外として認めている. 2 項の規定は通信の秘密の保護の観点から, 通信履歴の提供について厳格なルールを定めたものと考えられる.

### 4.1.4 通信履歴の保存期間

「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. (同上解説(5))」

ガイドライン解説では「一般に 6 カ月程度の保存は認められ」てはいるが，現状の保存期間は事業者の自主的な判断になっており，バラツキがあって統一されていない．

ログの保存期間を延長すると，サーバーなどのコストが増大するために，前 4.1.2 および 4.1.3 に述べられている規定への要請に応ずるとすれば，自己の必要性を超える期間のログの保存について，誰がそのコストを負担すべきかの問題は残っている．

## 4.2 ISP 等のパケット解析・ログの保存行為に関する法的解釈

ISP 等のパケット解析・ログの保存に関する議論は，「通信の秘密」の法解釈として論じられているので，以下の「通信の秘密」の観点から法的解釈を述べる.[32]

### 4.2.1 「通信の秘密」の観点からの ISP 等電気通信事業者の法的な位置づけ

憲法 21 条 2 項後段は，「通信の秘密は侵してはならない」と規定している．この「通信」というのは，「信書の秘密」と「電気通信の秘密」の両方を意味しているが，法律レベルでは，信書の秘密と電気通信の秘密に分かれて規定されている．

電気通信の秘密は電気通信事業法 4 条で，「電気通信事業者の取扱中に係る通信の秘密は，侵してはならない.」と規定されている．また同法 2 条で，電気通信事業者は「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」を営むものであって，運んでいる他人の通信にはノータッチで運ぶことを本来の任務としている．

地裁レベルの判決ではあるが，「電気通信事業者は，（中略）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」と判示している．（大阪地判平成 16.7.7 判時 1882 号 87 頁）

以上のように電気通信事業者は，発信者から受信者までノータッチで通信を届けることが，その本来的責務である．このため電気通信事業の従事者が通信の秘密を侵した場合の罰則は，それ以外の人が通信の秘密を侵した場合に比べて，刑罰が加重されており，通信の秘密を侵さないことが強く期待されているといえる．

電話が主な通信手段であった時代は，電気通信事業者（電話会社）が電話サービスを一元的に管理する仕組みであったことや，電気通信事業者の通信の秘密の遵守が職業倫理として徹底されていたこともあって，「通信の秘密」が侵される事例は極めて限定的であった．

---

[32] 4.2 項の「通信の秘密」に関する基礎的な事項，例えば「通信の秘密」の法体系,保障内容，「通信の秘密」の範囲，「通信の秘密を侵す」の意味，「電気通信事業者の取扱中に係る」の意義，電気通信事業者の「通信の秘密」に対する基本的な責務と電気通信事業者がその責務に反して，インターネット利用において「通信」に関与を求められるようになった背景・理由などについては，以下の文献を参照．

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 第 5 号 林紘一郎・田川義博[2012]「心地よい DPI(Deep Packet Inspection)と程よい通信の秘密」 情報セキュリティ総合科学第 4 号

### 4.2.2 通信に関与を求められるようになった電気通信事業者の関与の正当性の根拠

インターネット利用が主な通信手段となっている現在においては，サイバーセキュリティや違法有害情報の流通を防止するなどの必要性が高くなり，インターネットに関しては一元的な管理者がいないこともあって，それらのインターネットの負の側面に関する対策を実施するために，本来は通信にノータッチが求められる電気通信事業者が，自らが運んでいる通信に関与することが求められるようになっている．

関与は主としてインターネットの接続業務を行っているISP（Internet Service Provider）によって担われている．電気通信事業者が，他人の通信へ関与できる根拠については，現在は刑法理論に依拠している．

「刑法第 2 編 罪」において，どのような行為を行ったら罪となるかが定められていて，この行為類型が構成要素該当性といわれるものである．また構成要件に該当したとしても，違法性阻却事由がある行為や有責性がない場合には罪には問われない．

違法性阻却事由としては，以下の行為が該当する．

・正当行為(35 条) 法令または正当な業務による行為は罰しない．
・正当防衛（36 条） 急迫不正の侵害に対して，自己又は他人の権利を防衛するために，やむを得ずにした行為は罰しない．
・緊急避難（37 条） 自己又は他人の生命，身体又は財産に対する現在の危機を避けるため，やむを得ずにした行為は，これによって生じた害が避けようとした害の程度を超えなかった場合に限り罰しない．（以下略）

また通信当事者の同意がある場合にも，通信の秘密を侵したことにはならない．

### 4.2.3 電気通信事業者の関与を認めている法律とガイドライン

ISP 等がパケット解析等を行なった場合に，外形的には通信の秘密を侵す行為であっても，違法性が阻却される旨を規定した法律とガイドラインは，表 4 の通りである．

表4： ISP等がパケット解析を認められている例

| 法律・ガイドライン | 対象行為 | 関与の根拠 | 主な法益 |
|---|---|---|---|
| A:プロバイダ責任制限法 | 送信防止措置（アクセスブロック）<br>発信者情報開示 | 正当業務行為（法令） | 個人的法益 |
| B：迷惑メール防止法 | 送信ブロック | 受信者の同意<br>正当業務行為（法令） | 個人的法益<br>社会的法益 |
| C：青少年インターネット環境整備法 | 青少年閲覧防止措置<br>(法21条の用語) | 正当業務行為（法令） | 個人的法益 |
| D：自殺予告ガイドライン | 警察への発信者情報の開示 | 緊急避難 | 個人的法益 |
| E：サイバー攻撃等への対 | サイバー攻撃等の識別 | 正当業務行為 | 社会的法益 |

| | | | |
|---|---|---|---|
| 処のガイドライン | のためのパケット情報の取得 | 正当防衛<br>緊急避難 | |
| F:帯域制御の運用基準のガイドライン | 特定のアプリケーションのパケットを検知, 流通を制御 | 正当業務行為 | 社会的法益 |

注1：AおよびCの発信者情報は，通信傍受ではなく，掲示板やブログなどへの書込みの記録としての内容と送信元のIPアドレスを検査している.
注2：FにおけるP2Pファイル交換ソフトについては，アプリケーションのプロトコルが区々なので，ヘッダーとペイロードの両方の場合がある.
出典：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，情報セキュリティ大学院大学紀要，23頁．ただし，「C 青少年インターネット環境整備法」の項は追加．またEのガイドラインは現行の名称に変更.

# 5 サイバーセキュリティにおけるバルクデータの意義

## 5.1 総務省研究会の検討内容

総務省では,「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」での検討結果を, 2014 年 4 月に第一次とりまとめ, 2015 年 9 月に第二次とりまとめとして公表した. この研究会では，個別の攻撃手法を取り上げ，サイバー攻撃への対処策が正当化できるかを事例ごとに検討している. (正当化の考え方については 4.2.2 参照)

第一次とりまとめでは，① 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，② 新たな DDoS 攻撃である DNSAmp攻撃の防止，③ SMTP 認証を悪用したスパムメールへの対処，など 5 事例が取り上げられている.

第二次とりまとめでは，① C&C サーバー等との通信の遮断における有効な同意，② 他人の ID･パスワードを悪用したインターネットの不正利用への対処，③ DNS の機能を悪用した DDoS 攻撃に用いられている名前解決要求に係る通信の遮断について，など 4 事例が取り上げられていて，いずれの事例においても通信の秘密を侵害しない形での対応策が示されている.

違法性阻却事由があると判断する基準は，目的の正当性，行為の必要性および手段の相当性の 3 つをすべて満たしていることである. この検討手法では，サイバー攻撃への対処として ISP が外形的に通信の秘密を侵害する行為を行う場合において，通信の秘密侵害の度合い（法益侵害の程度）と，ISP の行為が守ることのできた法益の大きさを比較している.

守ることのできた法益には，サイバー攻撃を受けた利用者が侵害されるかもしれないプライバシー（個人的法益）とこの行為によって実現が期待される「セキュアで安定的なインターネット利用（社会的法益）の両方があると考えられる.

## 5.2 サイバー攻撃におけるバルクデータと特定データ

「電気通信事業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」（インターネットの安定的運用に関する協議会作成，初版:2007 年 5 月，現行第 4 版:2015 年 11 月）は, 5.1 の研究会のとりまとめ内容も取り込んで作成されている.

このなかには例えば，DNSAmp 攻撃を未然に防止するためには，「ISP のネットワーク網の入口又は出口において，そこを通過する全ての通信の宛先 IP アドレス及びポート番号を常時確認(下線は追加)」して，「特定のポートに対して送信された通信を割り出し（下線は追加），これを遮断」することの可否が検討されている．

総務省研究会やガイドラインの事例をみると，サイバー攻撃に対する防御策を講ずる場合には，上記の DNSAmp の事例のように全数のパケット解析によって，攻撃者の特定などを行うことが多いと考えられる．

シギント活動では，バルクデータを収集する場合と特定パケットを収集する場合があるが，以下その点を中心にして，サイバーセキュリティにおける法的課題を，章を改めて考察してみたい．

## 6 バルクデータの法的検討課題

(1) サイバー攻撃を行っている攻撃者の特定パケット解析を行う ISP の行為が正当化されるのは，違法行為者は違法行為を行っているが故に，「通信の秘密」の権利保護を主張できないからであり，これは違法な表現行為が表現の自由の権利保護の範囲外であることと同じである.[33]

(2) 問題は，違法行為を行っていない利用者のパケット解析も行うことに関してである．上記ガイドラインではこの行為にも，違法性阻却事由があると認められている．

(3) サイバーセキュリティ対策として，全数のパケット解析を行っても，通常は攻撃者などを特定する前段の自動的・機械的行為であって，攻撃者などが特定できれば，その他のログは ISP にとっては不要なものである．

このため通常は保存しないとすれば，「通信の秘密」の法益であるとされるプライバシー侵害の度合いは低いと考えられる．3.5.2 で述べたように，保存した場合に安全管理措置が不十分で漏洩した場合には，プライバシー侵害の恐れが高くなるが，そのようなケースは可能性が高くないと考えられる．

(4) サイバー攻撃の被害が深刻化し，重要インフラへのサイバーテロや企業や国家機密情報の窃取を目的としたサイバーインテリジェンスへとサイバーセキュリティの対象範囲が拡大している現状や将来を考えれば，セキュアで安定的なインターネット利用を可能にするような技術的，管理的，法制度的な対策を強化する必要がある．

通信の秘密などの観点から，ISP が行うサイバーセキュリティ対策は「行っても良い」行為と「行ってはいけない」行為に区分されている．しかし「セキュアで安定的なインターネット利用」を可能にするためには，ISP に「一定の行為を行うことを義務づける」ことも検討課題になるのではないかと考えられる．

というのも，サイバー攻撃では利用者も含め，最も脆弱性の高いところが攻撃されやすいので，インターネット全体を防衛するためには，脆弱性の高いところを底上げする必要があり，仮にボットネット化している PC などがある場合には，利用者に注意喚起するだけで

[33] 以下の文献の記述を参照．コンピュータへの不正アクセス者とは，保護されたコンピュータに権限なくアクセスする者であって，それゆえに，保護されたコンピュータとの通信においてプライバシーを合理的に期待できない者をいう．（石井夏生利[2014]『個人情報保護法の現在と未来』p260）

はなく，利用者の同意を得て，ISP なりどこかの組織が当該ボットネット化している PC からマルウエアを駆除するなどの対策も必要になると考えるからである．

(5) 現在の ISP の違法性阻却などの検討は，総務省研究会でも個別の事例ごとにその可否が検討されているが，巧妙化・複雑化するサイバー攻撃に対処するためには後手になりやすい．プライバシー・シールドの ANNEXⅡでは，EU 市民の個人データを米国に移転する場合の取扱いに関して，7 原則と補足的な 17 原則（Principles）が規定されている．この原則が明示されているので，これと比較することで現状評価ができる．また PPD-28 号 4 条において，最小化やデータセキュリティとアクセスのような，収集された個人情報の安全管理措置(safeguards)が規定されている．

日本においてバルクデータ利用が許容される場合であっても，プライバシーの原則や PPD-28 号の規定を参考に，適正な取扱いルールを定めることが望ましいと考えられる．このルール化，類型化によって個別判断によって後手になる事態を減少させることが出来るのではないだろうか．