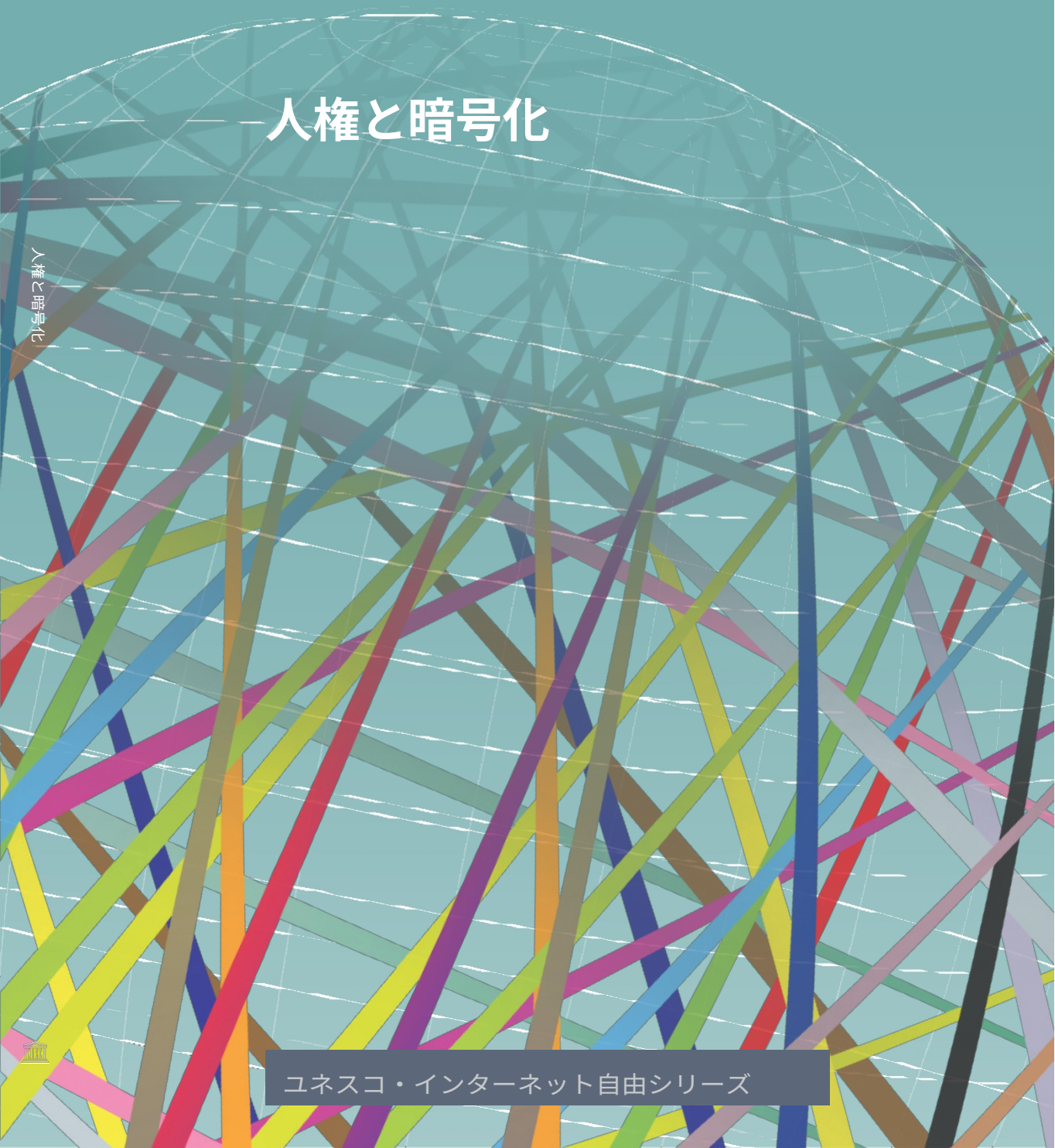
ユネスコ
出版

国際連合教育科学文化
機関

人権と暗号化

人権と暗号化



ユネスコ・インターネット自由シリーズ

ヴォルフガング・シュルツ ヨリス・ファン・ホーボケン

人権と暗号化

2016年、国連教育科学文化機関（UNESCO）により出版。所在地：フランス、パリ7区フォンテノワ広場7番地、
郵便番号75352。

ISBN 978-92-3-100185-7

著者は、各国報告書に関する校閲者およびその他の貢献者、ならびに研究支援に対して感謝する。校閲者：
- エドゥアルド・ベルトニ氏、アルゼンチン国家データ保護庁長官；
- デボラ・ブラウン氏、進歩的コミュニケーション協会（APC）、南アフリカ；
- ダニーロ・ドネダ氏、リオデジャネイロ州立大学、ブラジル；
- ジョセフ・ロレンツォ・ホール氏、CDT（民主主義とテクノロジーセンター）、米国；
- クリスティン・ランネガー氏、インターネット協会；
- ベン・ワグナー氏、欧州大学ヴィアドリーナ校インターネット・人権センター所長、ドイツ。

情報提供と情報源：
セダ・ギュルセス、イラ・ルビンスタイン、チンマイ・アルン、サルヴィート・シン、ジョシタ・M・パイ、エドゥアルド・マグラニ、ダニエル・カーン・ギルモア。研究補助：
フェリックス・クルパー、トビアス・マスト、ジュリアン・シュタベン。

ユネスコは、本出版物の発行にあたりドイツ連邦外務省の支援に感謝する。

Federal Foreign Office

表紙イラスト：© Shuttershock/greiss design

組版・印刷：ユネスコフランスで印刷

目次

はじめに

本書は、2015年11月の第38回大会で承認されたユネスコのインターネット問題に対する新たなアプローチに基づくものである。195の加盟国は、「CONNECTing the Dots」成果文書を採択するために採用した。この文書には、ユネスコによる今後の行動に関する38の選択肢が示されている。また、人権に基づく、オープンでアクセス可能なインターネットを提唱し、マルチステークホルダーの参加によって政府される「インターネットの普遍性に関する原則（R.O.A.M.）」も採択された。

この使命に沿い、ユネスコは国際プロセスやフォーラムを通じて関係者と継続的に連携し、安全、プライバシー、透明性、暗号化、情報源保護、ヘイトスピーチ、デジタル時代における過激化など、オンライン上の表現の自由に影響を与える課題への理解を深めるよう努めている。

本調査は、インターネット普遍性枠組みの実施に向けた取り組みの一環として作成された。具体的には、「CONNECTing the Dots成果文書」が推奨する選択肢、すなわちユネスコが「匿名性と暗号化がプライバシー保護と表現の自由の促進手段として果たし得る役割を認識し、これらの問題に関する対話を促進する」という提言にも応えるものである。

さらに、本研究は2015年6月に人権理事会に提出された、意見及び表現の自由の権利の促進と保護に関する特別報告者デイヴィッド・ケイの報告書を参考にしている。

暗号化は、現在のインターネットガバナンスに関する国際的な議論において重要なテーマである。本研究はこの主題を掘り下げ、様々な暗号化手段、その利用可能性、メディア・通信分野における潜在的なアプリケーションについて、世界的な概観を示す。暗号化の導入が、法やポリシーなどの異なる領域によってどのように影響を受けるかを説明し、選定された法域における暗号化の詳細な事例研究を提供する。メディア・通信環境における暗号化の役割と、各種サービス・組織・エンドユーザーへの影響を詳細に分析する。この調査・分析に基づき、多様なステークホルダーに有用な暗号化ポリシーに関する提言を行う。これには、現行議論におけるジェンダー感度の欠如への対応必要性の指摘や、「暗号化リテラシー」向上のためのアイデア提示も含まれる。

このインターネットの自由に関する主要出版シリーズは2009年に開始され、二つの主要な目的を有している。一つはインターネットの変容する法的・ポリシー課題を探求すること、もう一つはオンライン上の表現の自由をより促進する環境づくりに関心を持つ加盟国やその他の関係者に向けた提言を提供することである。

暗号化問題に関する国際的な対話と協力を促進する新たな知識資源としての役割に加え、私たちはさらに、この新版が以下の点で有用であることを期待する。

暗号化分野における知識、ポリシー選択肢、提言を、ユネスコ、加盟国、市民社会、民間セクター、学術界に提供することにも役立つことを願っている。

ユネスコは、この包括的かつ詳細な評価を提供してくれたヴォルフガング・シュルツ教授とヨリス・ファン・ホボケン博士に感謝の意を表する。また、草案をレビューし貴重な意見を提供してくれた国際的な専門家たちにも感謝する。

フランク・ラ・ルー

ユネスコ事務局次長

エグゼクティブ・サマリー

本調査は、情報通信分野において特に重要なテクノロジーである暗号化、より広くは暗号技術の利用可能性と使用に焦点を当てている。過去数十年間、暗号化技術はデジタル環境において他に類を見ない適性を発揮してきた。商業的、個人的、公共的利益のための情報通信保護を確保するため、様々な主体によって広く導入されている。人権の観点からは、関連する主体による暗号化技術の可用性と導入が、自由で開かれたインターネットを実現するための必要不可欠な要素であるとの認識が高まっている。具体的には、暗号化技術は表現の自由、匿名性、情報へのアクセス、私的通信、プライバシーを支援し得る。したがって、暗号化への制限は慎重に精査される必要がある。本研究は、メディア・通信分野における暗号化の人権関連性、干渉の合法性について論じ、国家の実践やその他の関係者に向けた提言を行う。

本出版物は、ユネスコのインターネット問題に対する新たなアプローチの文脈において、これらの問題を探求するものである。このアプローチは2015年11月に加盟195カ国によって採択するために採用され、先行大会「CONNECTing the Dots」の成果文書に基づいている。具体的には、ユネスコが「インターネットの普遍性」というこのコンセプトと関連する「ROAM原則」を支持することを意味する。これは（人権）に基づく、オープンでアクセス可能なインターネットがマルチステークホルダー参加によって政府されることを指す。

第2セクションでは、メディア・通信環境においてますます不可欠な要素となる暗号化技術の概要を説明する。サービスプロバイダーによる暗号化とエンドユーザーが直接使用する暗号化を区別しつつ、暗号化が保証し得る情報通信の多様な特性（機密性、プライバシー、真正性、可用性、完全性、匿名性など）を明らかにする。

第3セクションでは、電子商取引法、データ保護法、政府によるデータ・通信へのアクセス権など、情報法・ポリシーの様々な領域が暗号化テクノロジー・ソリューションの導入に与える影響を説明する。政府の合法的アクセスを目的とした暗号化バックドアの設計問題や、OECDガイドライン及び国連関連報告者の公式報告書を通じた国際的な規範形成の動向も考察する。

セクション4では、選定された法域（ドイツ、米国、インド、ブラジル、アフリカ地域）における暗号化ポリシーの現状について、より詳細な事例研究を提供する。これらの事例研究は、暗号化に対する制限（例：輸出管理する）の一般的な類型論の観点から見た暗号化ポリシー、ならびに暗号化の可用性と採用を促進するための積極的措置（例：データプライバシー規制におけるもの）の観点から暗号化ポリシーを検討する。選定されたいずれの管轄区域においても、暗号化の使用を全面的に禁止する規定は存在しない。しかし民間部門における暗号化ポリシーへの自由化の度合いには差異がある。具体的には、暗号化の正確な法的地位に関する重大な法的不確かさが存在し、これが事実上の使用制限として機能している。本研究ではさらに、政府の情報・通信アクセスを理由にインターネットユーザーの安全な暗号化利用を制限しようとする米国及び他地域における最近の提案についても論じる。

セクション5では、暗号化が人権およびメディア・通信に及ぼす影響を論じる。暗号化への制限は、国際的に保護されている表現の自由の権利および私生活の権利を侵害する可能性がある。本研究はこの点に関して、以下の3つの具体的な懸念視点を提示する。

第一に、暗号化は人々によって通信の完全性・可用性・機密性が保護されることで、抑制されない通信の要件を支える。この要件は通信の自由にとって重要な前提条件であり、国際レベルで強く認識される必要がある。

第二に、ポリシーや立法が暗号化とそのセキュリティ特性に制限をもたらす場合、透明性の原則を含む手続き上の保障が遵守されるべきだ。これは特に、国家が正式な措置を取らず、暗号化に影響を与える措置の実施を民間主体や業界の協力に依存する状況において重要である。

第三に、本調査はプラットフォーム上でユーザーの体験を保護する上で、仲介サービスプロバイダーの重要な役割を指摘する。具体的には、オンライン仲介業者はコンテンツやユーザー接続における仲介者としての役割だけでなく、セキュリティ仲介者としての役割も担っている。なぜなら、暗号化に関する彼らの慣行やデフォルト設定は、ユーザーがこれらのテクノロジーにアクセスし効果的に利用する上で極めて重要だからである。

第6セクションでは、関連する人権問題を適切に扱う上で有用な知見として、様々なステークホルダーに向けた提言を提示する。提言は政府、国際機関、技術コミュニティ、民間セクター、市民社会（ユーザーや学術界を含む）といった異なるステークホルダーグループと、彼らがシステム全体で果たす特定の役割を対象としている。提言の中で、本調査は暗号化に関する現行の議論や既存ポリシーにおけるジェンダー感度の欠如、脆弱なコミュニティの立場に対処する必要性を指摘している。

1. はじめに

研究の背景

「暗号技術は権力を再編成する。すなわち、誰が何を、何から行うことができるかを規定するのだ」[1]

私たちはそのテクノロジーが社会のかなりの部分を媒介する世界に生きている。情報通信テクノロジー、サービス、実践の分野における革新は、社会的な主体間の関係を再構築し続けている。そのアーキテクチャゆえに、これらの革新は情報・知識へのアクセス、プライバシーの保護、自由なコミュニケーションの能力といった基本的価値の促進につながる可能性がある。[2] 明らかに、テクノロジー設計に関する選択は、十分なエネルギー、時間、資源が投入されない場合や、その使用や展開を不当に制限するポリシーが採択される場合には、こうした価値の浸食や妨害をもたらす可能性もある。したがって、政策立案者やその他の利害関係者の課題は、アーキテクチャの設計を検討し、技術インフラのレベルで問題となる基本的価値の保護を確保することである。関連する利害関係者は、これらのテクノロジーが社会実践に組み込まれている以上、テクノロジーが発展を完全に決定づけるわけではないことも認識すべきだ。したがって、前述の現象を研究するにはテクノロジーを検討する必要があるが、そこで止まるべきではない。

本研究は、情報通信分野において特に重要なテクノロジーである暗号化、あるいはより広く暗号技術の利用可能性と使用に関連する人権的側面に着目する。(3)

暗号学は数学、計算機科学、工学の分野で古くから扱われてきた主題である。一般に「数学的手法を用いた情報と計算の保護」と定義される(4)。OECDガイドラインでは、暗号化と暗号学を以下のように定義している：

> 「暗号化」とは、情報の機密性を確保するため、暗号技術を用いてデータを不可解なデータ（暗号化データ）に変換することを意味する。
>
> 「暗号学」とは、情報の隠蔽、真正性の確立、改ざんの防止、否認の防止、および／または不正使用の防止を目的として、データを変換するための原理、手段、方法を体系化した学問を指す。(5)

1970年代以降、デジタルコンピューティングの普及と、いわゆる公開鍵暗号の発明により、暗号化は社会でより広く利用可能となった。それ以前は、強固な暗号化、すなわち解読が極めて困難な暗号化は国家主体の領域であった。しかし、過去数十年にわたり、暗号化技術とこの分野における継続的な革新は、デジタル環境での利用に特に適していることが証明されてきた。

---

1 Philipp Rogaway. The Moral Character of Cryptographic Work. University of California. December 2015. http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf.

2 例えば、レスィグ、ライデンバーグ、アッシャーら、バルキン、デナルディスを参照。

3 エド・フェルテン。ソフトウェアのバックドアとホワイトハウスNSAパネル報告書。2013年12月：「この二つの用語はしばしば同義語として使われるが、『暗号技術』はより広い技術的意味を持つ。例えば、デジタルシグネチャーは『暗号技術』であるが、技術的には『暗号化』ではないと言える」。https://freedom-to-tinker. com/blog/felten/software-backdoors-and-the-white-house-nsa-panel-report/.

4 Gürses and Preneel 2016.

5 OECDガイドライン。

暗号技術は、個人、商業、公共部門における情報と通信の保護を確保するため、様々な主体によって広く導入されている。暗号技術はまた、通信主体の匿名性を保護し、それによってより一般的なプライバシーを保護するためにも用いられる。

暗号化の普及と利用は、複雑で重要かつ激しい論争を伴う法的ポリシー論争を引き続き引き起こしている。1990年代には、国内および国際レベルで法的・その他の対立を伴う第一段階の議論が行われた。現在、世界は国際的・国内レベルで暗号化に関する第二段階の議論の真っ只中にあり、これは暗号化に関する既存のポリシー枠組みの更新が必要であることを示している。現在の第二の議論は、エドワード・スノーデンのメディアへの情報漏洩によって明らかになった政府の情報通信アクセス問題が引き金となった。それ以来、エンド・ツー・エンド暗号化ツールの開発とユーザーへの提供が著しく増加している。[6] 強力な暗号化は、メディアと通信環境において必要かつ有益な要素として広く認められている。OECD暗号ポリシーガイドラインの序文が指摘するように、暗号化は「国家およびグローバルな情報通信ネットワーク・テクノロジーの発展と利用、ならびに電子商取引の発展にとって極めて重要」である。[7] 暗号化は、ネットワークの安全性と完全性を促進するポリシー枠組みにおいて重要な役割を果たす。それでもなお、政府機関によるアクセスに潜在的な障害をもたらす可能性があることを理由に、その使用と展開を制限する必要性に関する政府声明や提案が存在する。本報告書の目的上、焦点は主に国家主体による合法的なアクセスに置かれ、悪意のあるハッカーなどによる一般的な不正アクセスには置かれない。政府アクセスを理由とした暗号化制限が、一般的な不正アクセス防止能力に深刻な悪影響を及ぼし得る事実は、当然ながら関連性がある。

同時に、国家主体・非国家アクターを問わず、国内外を問わず、法的手続き外の不正アクセス事例において暗号化が特に重要であることは確認されている。

こうした背景を踏まえると、業界関係者がここ数年、ユーザーの情報の通信保護を強化し、サービスへの信頼を促進するため、暗号技術の採用を大幅に拡大している点も指摘できる。この動向は適切に評価されるべきである。暗号化に関する様々な研究は、ビジネスモデルがユーザーデータに依存していることを考慮すると、関連業界関係者によるエンド・ツー・エンド暗号化の普遍的な採択はあり得ないと指摘している。[8] それにもかかわらず、エンド・ツー・エンド暗号化を提供する商用サービスの台頭と、法執行機関のアクセスを視野に入れた制限や解決策の要求が、暗号化の利用と、より一般的には暗号技術採用の法的地位をめぐる現在の議論に新たな燃料を注いでいる。

人権の観点からは、暗号化が自由で開放的かつ信頼できるインターネット実現の重要な要素であるとの認識が高まっている。これはユネスコにも当てはまる。ユネスコ刊行物『包摂的な知識社会を育むための基幹要素』[9]では、暗号化が議論され、今後の行動領域として特定されている。基幹要素

---

6 エンド・ツー・エンド暗号化とは、通信ツールやサービスに暗号化を適用し、そのツールやサービスのユーザーだけが平文メッセージにアクセスできるようにする手法を指す。詳細な議論についてはセクション2を参照のこと。

7 OECDガイドラインを参照のこと。

8 例えば、Soghoian 2009、Van Hoboken and Rubinstein 2014、Berkman Center 2016 を参照。

9 http://www.unesco.org/new/en/internetstudy を参照。

本研究は、「人々」が世界中の情報資源にアクセスできるだけでなく、地域社会や国際社会に情報や知識を提供できる、自由でオープンかつ信頼性の高いインターネット」というビジョンの確立に貢献することを目的とした。[10]このビジョンの実現に向けて、「匿名性と暗号化がプライバシー保護と表現の自由の促進手段として果たし得る役割」が認識されている。また、ユネスコの「これらの問題に関する対話を促進する」取り組みの価値も認められている。[11]本出版物は、2015年11月の第38回大会で承認されたユネスコのインターネット問題に対する新たなアプローチに沿ったものである。我々の195の加盟国は、「CONNECTing the Dots成果文書」を採択するために採用する。この文書には、ユネスコによる今後の行動に向けた38の選択肢が示されている。また、「インターネット普遍性原則（R.O.A.M.）」([12]も採択する。これは、人権に基づく、オープンでアクセス可能なインターネットを提唱し、マルチステークホルダー参加によって政府されることを主張するものである。

意見及び表現の自由の権利の促進と保護に関する現職及び前任の国連特別報告者も、情報通信分野における人権実現の手段として暗号化を認めている。当時の報告者フランク・ラ・ルーは、2013年の報告書「国家による通信監視がプライバシー権及び意見及び表現の自由の権利の行使に及ぼす影響」において、次のように結論づけた。

> 国家は、通信サービスのプライバシー、安全性、匿名性を損なう措置を民間企業に強制してはならない。これには、国家監視目的のための傍受能力構築の要件や暗号化使用の禁止も含まれる。[13]

その後任である国連特別報告者デイヴィッド・ケイは、デジタル時代における意見及び表現の自由の権利行使のための暗号化と匿名性の利用を評価する報告書を特に作成し、2015年6月に人権理事会に提出した。[14]ケイは、暗号化と匿名性はプライバシー権及び表現の自由の権利の下で保護されるべき地位に値すると指摘した：

> 暗号化と匿名性は、現代のオンラインセキュリティにおける主要な手段であり、個人にプライバシー保護の手段を提供する。これにより、干渉を受けずに意見や情報を閲覧・読解・形成・共有する能力が力づけられ、ジャーナリスト、市民社会組織、民族・宗教集団の構成員、性的指向やジェンダーゆえに迫害される者、活動家など、意見及び表現の自由の権利を行使できるようになる。[15]

本報告書はまた、人権との関連性、干渉の可能性の合法性に関するこの質問にも言及し、国家の実践やその他の関連する利害関係者に対する提言を行った。[16]

---

10 UNESCO. 包括的な知識社会を育むための基盤. パリ 2015. http://unesdoc.unesco.org/ images/0023/002325/232563E.pdf.

11 同上、66頁。

12 ユネスコの「Connecting the Dots」成果文書とインターネット普遍性に関する概念論文は、本出版物の付録として添付されている。

13 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement

14 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

15 デイヴィッド・ケイ。意見及び表現の自由の権利の促進及び保護に関する特別報告者の報告書。2015年5月。http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/ Documents/A.HRC.29.32_AEV.doc。

16 詳細な議論については、セクション3を参照のこと。

研究疑問、範囲及び目的

以上のことから、メディア・通信分野における人権支援手段としての暗号化技術について、情報に基づいた国際的議論の中立的な基盤となり得る研究が、貴重な貢献を果たし得ることは明らかである。特に、国内および国際レベルで進行中の議論を結びつけ、業界関係者の役割を検討することには大きな価値がある。この目標を推進するため、本研究では以下の主要な疑問に取り組む：

- メディア・通信環境における暗号化テクノロジー・ソリューションの導入状況は、関連業界関係者およびエンドユーザーコミュニティ全体で現在どの程度進んでいるか？（セクション2）
- 情報法やポリシーの異なる領域が、暗号化テクノロジーとソリューションの導入にどのような影響を与えているか？（セクション3）
- 暗号化に対する制限と積極的措置の一般的な類型論を通じて見た、アフリカ地域を含む五大陸の選定された管轄区域における暗号化ポリシーの現状はどうか？（セクション4）
- 暗号化テクノロジーとソリューションの導入は、メディア・通信分野における人権保護とどう関連しているか？（第5セクション）
- 暗号化の文脈において人権尊重を最も効果的に確保できる政策選択肢とステークホルダーの行動は何か？（第6セクション）

これらの疑問を詳細に検討する前に、定義と本調査の一般的な範囲について少し時間を割く価値がある。結局のところ、本調査は、人権保護、特に国際レベルで保護されているプライバシー権と表現の自由の権利を支える暗号化の役割に関する議論を促進することを目的としている。最近の報告書で指摘されているように、匿名性を確保する措置は、これらの権利を支える上で暗号化と同様の役割を果たすことが観察される。しかし混乱を避けるため、本研究では一貫して、問題となる規範的価値（例：個人の情報・通信の保護、情報へのアクセス保護）と、これらの価値を保護する可能性のあるテクノロジー（暗号化、認証、難読化）を区別する。さらに、利用可能な選択肢の多様性を考慮し、問題となる具体的な暗号技術を一貫して明確化する。

上述のように定義される暗号化は、情報と計算を保護するための暗号技術の一部に過ぎない。しかし暗号化の規範的価値は固定されたものではなく、使用または展開される暗号手法の種類や目的に応じて変化する。伝統的に暗号化（暗号化）技術は、通信の機密性を確保し、意図された受信者以外の者による情報や通信へのアクセスを防止するために用いられてきた。これが今日の暗号化論争で最も一般的な用途であり、本研究の主たる焦点である。しかしこれは暗号技術の一部に過ぎない。暗号技術は通信当事者の真正性や通信内容の完全性を保証し、デジタル環境における信頼を可能にする重要な要素を提供する。別の技術群は*メタデータの*保護に関わり、インターネット及びインターネットベースの特定サービス利用者の匿名性保護を含む。

したがって、本研究は人権と暗号化の接点における諸問題を、以下の観点から検討する。最終的に重要なのは

「暗号化」そのものや特定の暗号手法ではない。人権の観点で重要なのは、機密性、プライバシー、真正性、可用性、完全性、匿名性といった、人間が関わる通信（および情報）の特性が確立され、それらが妨害される可能性である。暗号手法は重要であり、その使用や展開への干渉は慎重に検証されるべきである。なぜなら、これらの手法はインターネットのような信頼できない通信プラットフォーム上でも、重要な特性を技術的に保証するからである。例えば、インターネットアクセスプロバイダーがエンドユーザー間のトラフィックを暗号化しない場合でも、通信アプリケーションは暗号化プロトコルを実装し、通信の「機密性」という特性を保証できる。

暗号化は、個人情報や通信に対するユーザーの制御を強化するために利用され得る。本研究では、この種の利用に焦点を当てる。具体的には、エンドユーザー向けツールやアプリケーションの利用可能性、コミュニティ主導プロジェクトの重要性を認識しつつ、様々なサービスや組織がユーザーデータのセキュリティ保護と人権支援のために暗号化をどのように利用・展開しているかに特に重点を置く。ここで留意すべきは、暗号化が人々に対して危害を及ぼしたり、アクセスすべき情報へのアクセスを妨げたり、利用可能なツールの使用を阻害したりする手段にもなり得る点だ。例として、攻撃者が鍵を保持し身代金と引き換えにのみ開示する方式でユーザーのデバイスを暗号化する「デバイス暗号化攻撃（ランサムウェア）」が挙げられる。別の例としては、情報へのアクセスやコミュニケーションに不釣り合いな影響を与える形で、デジタル著作権管理（DRM）が不当に制限的に使用されるケースがある。

暗号化の人権への影響を議論する際、特に注目すべきコミュニティが存在する。例えば政治活動家やジャーナリスト、そして彼らが所属する関連機関や組織である。暗号化の人権上の受益者が誰であるかを考える際、これまでの暗号化に関する議論の多くがジェンダーに無関心であったこと、あるいはさらに悪いことに男性中心であったことに留意すべきだ。オンライン空間において、女性と女子が表現の自由、プライバシー、尊厳、安全に関する権利の侵害を特に受けやすいことは広く認識されている。[17] 暗号化技術が女性と女子、脆弱なコミュニティの保護を促進し得る点は注目に値する。この点に関する詳細な分析を提供するため、さらなる研究と調査が明らかに重要な課題である。一般的に、人権と暗号化に関する広範な社会的議論は、標的型監視や関連する人権侵害の被害者たちの経験からも学ぶものとする。これには人種的・民族的・宗教的少数者、ジャーナリスト、ブロガー、女性と女子、LGBTコミュニティなどが含まれる。[18]

暗号化（およびその制限必要性の主張）に関する継続的な議論を追ってきた者なら、虚偽の議論が繰り返される傾向に気づかざるを得ない。暗号化の利点は文脈に置く必要がある。そうしなければ、暗号化自体の利点は誤解されたり、文脈において期待される保護を提供しない可能性がある。例えば、通信当事者間の通信を暗号化しても、アクセス権を持つ当事者が情報を第三者に渡すことを防げない。残念ながら、暗号化は意図せず注目を集めたり、疑念を生じさせたりする可能性もある。

---

17 例：ユネスコ『ユネスコ、女性と少女に対するオンライン・オフラインの暴力対策を求める』2015年9月25日。参照先：http://www.unesco.org/new/en/communication-and-information/resources/news-and-in-focus-articles/all-news/news/launch_of_the_broadband_commissions_report（最終アクセス日：2016年9月14日最終アクセス）。

18 例えば、Gürses, S., Kundnani, A. and Van Hoboken, J., 2016. Crypto and empire: the contradictions of counter-surveillance policy advocacy. *Media, Culture & Society*, 38(4), pp. 576-590.

人権の効果的な享受を損なう形で、特に一般的な法の支配による保護が欠如している状況において。したがって、暗号化を使用する可能性そのものは、自由な通信を保障する十分な手段とはならない。

逆に、政府関係者が通信を復号する権限から得られる利点に関する仮定も、厳密な検証に値する。第一に、そのような権限を実装する技術的課題には重大な疑問がある。仮に実現したとしても、計画された違法行為に関する通信は、一見日常的で無害な言葉遣いを通じて、平然と隠蔽される可能性がある。第二に、情報または通信へのアクセスを妨げる暗号化の役割は、利害関係者によって著しく過大評価されているかもしれない。おそらく暗号化の数学的性質こそが、その保証の一部を絶対的なものに思わせる所以だろう。しかし必要とあれば、国家機関や犯罪者は暗号化技術を回避・迂回する多様な手段（実装上の欠陥やサイドチャネルの悪用など）を駆使できる。特定の国家機関が有する資源と計算能力は、多くの高度な暗号化テクノロジーでさえ最終的に防御を破られる可能性があるほどである。さらに、より安全な情報通信ツールを使用している場合でも、ユーザーは複数の方法で脆弱な状態に置かれる可能性がある。この実例として、昨年の香港抗議活動において、攻撃者がWhatsappを利用してユーザーを非安全なアプリケーションへ誘導した事例が挙げられる。[19] Hacking Team文書の最近の開示によって明らかになった情報は、市民社会、ジャーナリスト、活動家に対してこうした手段を用いる市場が出現していることを示している。[20] こうした動向は、ネットワーク化された世界において人々や機密情報を保護するには、暗号化は必要だが十分ではないことを示唆している。また、暗号手法やテクノロジーを取り巻く開発の加速化も示しており、これらの問題に関する包括的な発言やポリシーには警戒すべきである。

2. メディア・通信分野における暗号化

以下は、メディア・通信環境における関連暗号技術の最新動向を簡潔に概説するものである。本文では特定の暗号手法とアプリケーションを参照し、重要な区別を明確化すると同時に、技術的知識を持たない読者にも理解可能な表現を心がけている。特に重点を置くのは、サービスプロバイダーによる暗号技術の実際の導入・運用状況、ならびに個人や関連専門家が実際に利用可能な状況に関する進展である。

これらの議論において、以下の二つの根本的な区別が中心となる。[21] 第一に、暗号化の導入責任主体に基づく区別である：暗号化はサービスプロバイダーの選択の結果として使用されるのか、それとも（インターネットユーザーの）コミュニティによって導入されるのか？ユーザー側またはクライアント側の暗号化ツール・テクノロジーによる展開を議論する際には、人権の観点から関連する特別なセキュリティニーズを持つユーザーコミュニティ、例えば人権活動家などを念頭に置くことが重要である。

19 ジム・フィンクル。香港抗議者を標的とした高度なiOSウイルス - セキュリティ企業、ロイター通信、2014年9月。http://www.reuters.com/article/hongkong-china-cybersecurity-apple-idUSL2N0RV2D320140930（最終アクセス日：2016年9月14日）。

20 アレックス・ハーン。ハッキングチームがハッキング被害：抑圧的な政権にスパイツールを販売していたと文書が主張。*ガーディアン*。2015年7月6日。http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim (アクセス日: 2015年12月14日)。

21 アイラ・ルービンスタインとヨリス・ファン・ホーボケンに続く。クラウドにおけるプライバシーとセキュリティ。メイン・ロー・レビュー 2014年、pp. 488 et seq. および Claudia Diaz, Omer Tene, Seda Gürses. ヒーローか悪役か：プライバシー法とテクノロジーにおけるデータ管理者, 74 (2013) オハイオ州立大学法学ジャーナル, pp. 923 et seq.

人権擁護活動家、社会的弱者、ジャーナリスト、その他のオンラインメディア関係者。

第二の区別は、エンド・ツー・エンド暗号化とその他の暗号化手法との違いである。サービスプロバイダーにユーザー情報へのアクセス提供を法的に強制する可能性という核心的問題を考慮すると、特に暗号化の人権への影響を検討する際に重要な区別となる。多くの暗号化は、サービスプロバイダーが通信を保護するために導入されるものであり、これにより*第三者の*不正アクセスは防止されるが、それを実装したサービスプロバイダーは依然として関連するユーザーデータにアクセスできる。エンド・ツー・エンド暗号化とは、*サービスプロバイダー自身も*ユーザーの通信にアクセスできないようにする暗号化を指す。こうした暗号化方式の実装が、最近最も議論を呼んでいる。

サービスプロバイダーが導入する第三者不正アクセス防止技術

最も広く導入されている暗号技術の一つは、インターネットユーザーと特定サービスプロバイダー間の通信経路を不正な第三者のアクセスから保護する技術である。これらの暗号技術は、ユーザーとサービスプロバイダーが共同で運用しなければ機能しない。つまり、オンラインニュース出版社やソーシャルネットワークなどのサービスプロバイダーが、サービス設計と実装に積極的に組み込む必要がある。ユーザーはこれらの技術を単独で導入できず、その導入はサービスプロバイダーの積極的な参加に依存する。

例えば、電子銀行やオンライン図書館などのウェブサービスプロバイダーは、ユーザーとの通信を保護することを決定できる。サービスプロバイダーは、いわゆるトランスポート層セキュリティ（TLS）標準に依存することでこれを実現できる。TLSは、クライアントとサーバー間の通信をあらゆる第三者から*秘密に*保つことをサービスプロバイダーに可能にする。特に注目すべきは、通信当事者（通常はサーバーのみ）の認証と通信内容の改ざんチェックを双方に可能にする点だ。([22])TLSが有効化されると、ユーザーは銀行ログイン情報を実際の銀行に提供していると信頼できる。ニュースサイトを訪れる読者は、改ざんされた記事を読んでいないと信頼できる。

HTTPSヘッダーを通じて一般インターネットユーザーに可視化されるTLSプロトコルは、オンライン商取引、電子政府サービス、医療アプリケーションのセキュリティ確保に広く利用されている。また、ルーターやカメラなどネットワークインフラを構成するデバイスにも適用される。しかし、この標準規格が確立されてからほぼ20年が経過しているにもかかわらず、テクノロジーの普及と進化は遅く、近年になってようやく顕著な進展を見せている。

他の暗号化手法やプロトコルと同様に、適切かつ安全な（より広範な）導入に関連する実務上の課題は重大であり、考慮する必要がある。多くのサービスプロバイダーは依然としてTLSを実装していないか、適切に実装していない。多くのサーバーは、デフォルトで、あるいは全く、TLSを用いた安全なプロトコルバージョンを提供していない可能性がある。さらに、サーバーはセッションごとに鍵を切り替え使用済み鍵を破棄する代わりに、長期間同じ暗号鍵を使い続ける選択をするかもしれない。後者のバージョンは完全前方秘匿性と呼ばれ、一般的にベストプラクティスと見なされている。これは、ある鍵が漏洩しても、それ以前に暗号化されたデータが復号されないという利点がある。

---

22 参照：Eitan Konigsburg. Embracing HTTPS. 2014年11月. http://open.blogs.nytimes. com/2014/11/13/embracing-https/ (最終アクセス日: 2016年9月14日).

それでもなお、多くの実装では長期鍵に依存している。

ユーザーとインターネットサービス間の通信を保護する暗号化は、悪意ある第三者に対するユーザーのプライバシーとセキュリティを大幅に改善する。大量監視プログラムに関する最近の暴露は、関連企業がユーザーとサーバー間の通信を保護しない場合、世界中の政府機関が通信データを大量に収集できる現実を再認識させた。[23]この状況はその後、大幅な変化を遂げている。多くの企業は、データへの不正アクセスを想定し、サービスのセキュリティ強化のためにTLS類似のソリューションを導入している。([24]) 公開事例の中には、サービスプロバイダーのデータセンター間や異なるプロバイダー間の通信データも保護対象に含まれるものがある。市民社会団体は主要サービスのTLS導入状況を公に監視し始めた。例えばEFFの「Encrypt the Web Report」を参照のこと。([25])Googleは透明性レポートの特別セクションで、ウェブ上位100サイトのHTTPS導入状況を監視している。([26])

TLSの普及拡大は、ジャーナリスト[27]や市民社会団体、その他機関にとって特に価値がある。これらはユーザーや情報源との機密通信を重視し[28]、読者にコンテンツを提供する際、盗聴や内容を操る不必要なリスクに晒さないためだ。HTTPSに移行した主要サービスプロバイダーのリストには、Twitter、Facebook、Google検索、Gmail、Tumblr、そして最終的にはYahoo!も含まれており、10億人以上のユーザーが影響を受ける。

第三者からの通信保護に向けた暗号化導入には顕著な改善が見られる。しかし研究や調査が示すように、セキュリティ対策の導入・維持は、全てのオンラインサービスが習得を望み、かつ習得できる技術ではない。さらにTLSへの注目度上昇に伴い、関連プロトコルにおける大規模な脆弱性（例：HeartbleedやFREAK攻撃）が表面化した。[29] こうした脆弱性の出現は、暗号化による通信の安全性を確保・維持するためには、関連技術専門家コミュニティによる世界的な協調的かつ継続的な取り組みが必要であることを浮き彫りにした。Let's Encryptのような取り組みは、実装の容易さを含め、こうした課題の一部に対応している。[30]

無線通信の文脈においても、通信を第三者から保護する暗号技術の利用は重要である。無線通信を保護するため、様々な規格が開発されてきた。携帯電話、基地局、基地局コントローラ間の通信のための2G、3G、4G規格。モバイルデバイスと無線ルータ（「WLAN」）間の通信を保護する規格。そして

---

23 インターネットアーキテクチャ委員会（IAB）による規格。広範な監視下における機密性：脅威モデルと問題定義。2015年8月。http://tools.ietf.org/html/rfc7624。背景と議論についてはArnbak 2016を参照のこと。

24 Van Hoboken と Rubinstein の同上も参照のこと。

25 電子フロンティア財団。EFFのウェブ暗号化レポート。2014年11月。https://www.eff.org/.encrypt-the-web-report（最終アクセス日：2016年8月29日）。

26 Google, 透明性レポート, 主要サイトにおけるHTTPS, https://www.google.com/transparencyreport/https/grid/?hl=en.

27 Kevin Gallagher. なぜより多くの報道機関がSTARTTLS暗号化で電子メールを保護しないのか？. 2015年2月24日. https://freedom.press/blog/2015/02/why-arent-more-news-organizations-protecting-e-mail-with-starttls (最終アクセス日: 2016年8月29日).

28 情報源について、ジャーナリストは通常、通信内容の機密性保護に加えて、匿名性の保護を求める。これにはメタデータに関連する追加対策が必要となる。

29 https://freakattack.com（最終アクセス日：2016年8月29日）を参照。

30 https://letsencrypt.org（最終アクセス日：2016年8月29日）を参照。

ローカルコンピュータネットワーク。無線セキュリティ規格の初期バージョンには脆弱性があったが、最近のバージョンでは大幅な改善がなされている。[31]

これらの設計における一般的な弱点は、無線通信の送信ポイント（例：通信事業者）が全通信にアクセス可能であることだ。[32] この脆弱性は、無線プロトコルがユーザーデバイスのみを認証し、無線アクセスポイントを認証しない場合に悪化する。例えば初期の移動体通信規格（ GSM）では、携帯電話のみが認証対象であり、接続先の基地局は認証されない。悪意のある者や政府機関はこの弱点を利用し、偽の基地局を設置することで通信を傍受し、特定場所の移動体ユーザーを追跡できる。こうした偽基地局は一般に「IMSIキャッチャー」と呼ばれる。([33, 34, 35])

家庭などのローカル環境における無線技術の普及に伴い、「モノのインターネット（IoT）」の台頭により無線セキュリティの疑問は緊急性を増している。モノのインターネットとは、コンピュータだけでなく、ますます多くの物体（およびそれらに設置されたマイクやカメラなどのセンサー）がインターネットに接続されるという発展を指す。人々が行動し、環境情報を収集しネットワークと通信する日常的な物体に囲まれるようになると、無線システムにおけるセキュリティとプライバシー対策の有無はさらに重要になる。([36]) 最近のバークマンセンターによる暗号化に関する研究が指摘するように、モノのインターネットは監視の新たな経路を開く可能性がある。これはまた、「暗号化された経路を監視できない場合でも、別の経路を通じて遠隔から個人を監視する能力によってその弱点が補える」ことを意味する。([37])

前述の技術は、転送中または保存中のユーザー情報を第三者から保護できる。これらの技術は両方の段階で異なる形で適用される場合もあれば、一方の段階のみに適用される場合もある。「保存時」の定義には、データがデバイスに保存されているか、クラウドのようなローカルサーバーに保存されているかの違いもある。例えば携帯電話は盗難に脆弱であるため、サービスプロバイダーによるアクセスさえ制限することに特に注意を払う必要がある（後述）。一般的に、サービスプロバイダーが他の商業組織や政府などの第三者にこの情報を開示する可能性は排除されない。つまり、ユーザーはサービスプロバイダーが自らの利益のために行動すると信頼する必要がある。サービスプロバイダーが法的強制によりユーザー情報を引き渡す、あるいは特定のユーザーとの通信を妨害する可能性は残る。次のセクションでは、サービスプロバイダー自身がユーザーの入力内容にアクセスできないようにする方法について私たち論じる。ユーザーの通信内容にアクセスしないと謳って営業するサービスも存在する。

---

31 GSMMapは、これらの対策の実施状況について、国別・通信事業者別に概要を提供している。詳細はhttp://gsmmap.orgを参照のこと（最終アクセス日：2016年8月29日）。

32 Gürses and Preneel, 2016.

33 ACLU. スティングレイ追跡デバイス：誰が所有しているのか？. https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (最終アクセス日：2016年8月29日).

34 Eric King and Matthew Rice. 時代遅れ：英国はいつIMSIキャッチャーの存在を認めないふりをやめるのか？ 2014年11月5日。https://www.privacyinternational.org/node/454（最終アクセス日：2016年8月29日）。

35 ダン・グッディン。4G/LTEネットワーク向け低コストIMSIキャッチャーが携帯電話の正確な位置を追跡、arsTechnica。2015年10月28日。http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/ (最終アクセス日: 2016年8月29日)。

36 Yulong Zou, Xianbin Wang and Lajos Hanzo. 無線セキュリティに関する調査：技術的課題、最近の進展、将来の動向。IEEEプロシーディングス。2015年5月。http://arxiv.org/pdf/1505.07919.pdf。

37 バークマンセンター 2016年。

サービスプロバイダーが導入した技術は、サービスプロバイダーのアクセスを制限するものである。

サービスプロバイダーは、情報と通信へのアクセス能力を制限する措置を講じることもできる。これにより、ユーザーの情報と通信へのアクセスに対する保護がさらに強化される。こうした措置（プライバシー強化テクノロジー：PETsとも呼ばれる）の完全性は、繊細な設計上の決定と、サービスプロバイダーが透明性と説明責任を果たす意思に依存する。プライバシー強化テクノロジーは、サービスプロバイダーがアクセス可能なあなたのデータを最小限に抑えつつ機能を提供するように設計されている。最も普及している例は現在、プライベートメッセージング市場で見られる。

まず留意すべきは、こうしたサービスの多くにおいて、サービスプロバイダーは（通信機能以外に）連絡先リスト管理といった追加機能を提供し得る点だ。つまり、誰が誰と通信しているかを観察できるが、メッセージの内容は読めないよう技術的措置を講じている。これはユーザーにとって潜在的に悪影響を及ぼす。例えば、サービスプロバイダーは、サービスを利用して通信したいユーザー同士を接続する措置を取らなければならないため、そもそもユーザー間の通信を阻止する権限も持つことになる。

現在のプライベートメッセージングサービスは、採用される暗号化技術において急速に変化している。設計上の非常に微妙な差異が、特定のアプリケーションのプライバシー保証に重大な影響を与える可能性がある。FacebookのWhatsAppとAppleのiMessage[38]は、大規模なプライベートメッセージング展開の例である。しかし両サービスとも、セキュリティ設計上、FacebookとAppleが提供する追加機能を利用することで、理論上は暗号化されていない通信の傍受を支援する手段を保持できる状態だった。([39] [40]) 厳密な意味では、この点が両アプリケーションをエンドツーエンドのプライベートで安全な通信プロバイダーとして分類する資格を欠く要因となっていた。最近、WhatsAppはエンド・ツー・エンド暗号化の導入を完了し、現在では（10億人を超える）全ユーザーのデフォルト設定となっている。([41])WhatsAppはエンド・ツー・エンド暗号化の技術的実装に、Open Whisper Systemsが設計したSignal Protocolを採用している。([42])

微妙な技術的差異がユーザーの保護に重大な影響を及ぼし得ることを考慮すると、セキュリティやプライバシーの保証を提供するサービスを名乗るものに対して、透明性と技術監査を求めることは、セキュリティ・プライバシー工学コミュニティにおける一般的な慣行である。この点で模範的なサービスも存在する。例えば、オープンソースプロジェクトおよび企業であるOpen Whisper SystemsはSignalエンドツーエンド暗号化を提供しており、そのコードは公の監視に公開されコードレビューも受けているため、その有効性を検証できる。([43]) 脆弱性の発見を受けて、フリーでオープンなソフトウェアコミュニティから生まれる広く利用されるコードの監査に、より多くの投資が必要であるという認識が高まっている。

---

38 Apple, Our Approach to Privacy, http://www.apple.com/privacy/approach-to-privacy/.

39 Joseph Cox. Apple's iMessage Defense Against Spying Has One Flaw. Wired. 2015年9月8日. http:// www.wired.com/2015/09/apple-fighting-privacy-imessage-still-problems/ (最終アクセス: 2016年8月29日).

40 ファビアン・シェルシェル。WhatsAppの暗号化を監視する。c't。2015年4月30日。http://m.heise.de/ct/artikel/Keeping-Tabs-on-WhatsApp-s-Encryption-2630361.html（最終アクセス日：2016年8月29日、2015年）。

41 Cade Metz,「Apple対FBIは忘れろ：WhatsAppが10億ユーザーに暗号化を適用」2016年4月5日。http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/

42 WhatsApp, WhatsApp暗号化概要, 技術ホワイトペーパー, 2016年4月4日.

43 EFF. セキュアメッセージング評価表。2015年11月3日版。https://www.eff.org/secure-messaging-scorecard (最終アクセス日: 2016年8月29日)。

通信の保護に加え、サービスプロバイダーは、暗号化されていないデータにアクセスできない方法で、保存中のデータを保護する役割も果たす可能性がある。現在では多くのユーザーが複数のデバイス（ノートパソコン、携帯電話、ディスクドライブなど）を管理しており、これらは紛失、盗難、売却される可能性がある。追加対策が講じられていない場合、デバイスにアクセスできる者は誰でも、これらのデバイスに保存された情報を抽出できるかもしれない。このような情報漏洩は、デバイスの所有者だけでなく、デバイスに情報が保存されていた他の関係者全員にとって重大な結果をもたらす可能性がある。

デバイス上の情報を保護するため、認証付き暗号化を適用できる。デバイス暗号化の採択は従来限定的で、暗号化を有効にする能力やその可能性を認識しているユーザーは少なかった。近年ではGoogle ではやAppleを含む関連企業が、デバイス暗号化機能の強化を開始している。[44] ここでも鍵の保管場所に関する設計上の判断が重要となる：デバイス上に鍵を保存しても、デバイスへのアクセス権を持つ、あるいは入手可能な攻撃者に対しては効果的でない可能性が高い。[45] 特にAppleのデバイス暗号化は注目に値する。これは法執行機関のアクセス権限への影響を巡り、国際的にも大きな議論を巻き起こした事例である。AppleとFBIの間で広く議論された事例――Appleにデバイスロック解除の回避策作成を強制できるか否か――は、暗号化論争における対立する立場間の複雑さと共通理解の欠如を浮き彫りにした。([46] 新たな対策が政府機関に問題を引き起こす場合もあるが、ユーザーデータがクラウドと同期される傾向にある事実がこうした懸念を緩和している。([47]

業界関係者は、端末の管理や紛失がユーザーにとって問題であることを認識している。そのため、機密性の強調よりも、ユーザーデータのシームレスな可用性を通じたサービス継続が主要な関心事となる傾向がある。結果として、サービスプロバイダーは現在、ユーザーデータをクラウドに複製することで、端末管理や紛失に関する問題に対処するのが一般的だ。クラウドへのデータ保存は、時間やデバイスを超えた可用性を保証する一方で、強制やハッキングによる第三者のアクセスリスクを高め、サービスプロバイダーによる利用やプロファイリングを可能にする。またクラウド保存時、認証付き暗号化がユーザーに完全かつ効果的な保護を提供する条件は、復号鍵がクラウドではなくデータ所有者が管理するローカルに保管されている場合に限られる。

ユーザーデータの収集・処理に依存するビジネスモデルの普及は、保存状態の情報を保護する暗号化メカニズムを採択するために妨げる要因となり得る。実際、ブルース・シュナイアーが指摘したように：

---

44 サミュエル・ギブス. 地方検事「Googleは一部のAndroidデバイス を遠隔でロック解除可能」. ガーディアン. 2015年11月24日, http://www.theguardian.com/technology/2015/nov/24/google-can-unlock-android-devices-remotely-if-phone-unencrypted (最終アクセス: 2016年8月29日).

45 アンディ・グリーンバーグ。警察はiPhoneに侵入するために暗号化のバックドアを必要としない。2015年10月12日。http://www.wired.com/2015/10/cops-dont-need-encryption-backdoor-to-hack-iphones/ (最終アクセス日: 2016年8月29日)。

46 詳細な議論については、セクション3およびセクション4を参照のこと。

47 マイカ・リー。Appleは依然として連邦当局に提供できるあなたのデータを大量に保有している。The Intercept. 2014年9月22日。https://theintercept.com/2014/09/22/apple-data/（最終アクセス日：2016年8月29日）。特に、データがクラウドに保存されている場合、法執行機関がアクセスを得る上で固有の課題が生じうる。例えば参照：サイバー犯罪条約委員会（T-CY）『クラウド上のデータへの刑事司法アクセス：課題』ディスカッションペーパー、フランス・ストラスブール、2015年5月26日。

「監視はインターネットのビジネスモデルだ。これは驚くほど広範で堅牢、かつ収益性の高い監視アーキテクチャへと進化した。インターネット上では、多くの企業やデータブローカーによって、行く先々でほぼ追跡されている。あるサイトでは10社、別のサイトでは12社といった具合だ」[48]

その結果、クラウドアプリケーションを通じてユーザーのプロファイリングに依存する商用サービスプロバイダーが、エンド・ツー・エンド暗号化を広く導入する可能性は低い。しかし、暗号技術の最近の進歩により、「暗号化された領域」で一部のサービスを提供することが可能になった。例えば、高度な暗号技術を用いれば、暗号化されたデータを検索できる。検索語句が事前に分かっている場合、暗号化は安全でありながら、暗号文内で検索語句を探すことができるようにデータを暗号化できる。これは「プライベート情報検索」とも呼ばれるサービスだ。さらに進歩した技術では、暗号化されたデータに対して他の操作を行うことも可能かもしれない。いわゆる同型暗号の進歩により、サービスプロバイダーは暗号化されたデータ上で計算を実行できるが、結果を復号できるのはユーザーだけである。[49]

最後に、暗号技術はオンライン上の本人確認管理において重要な役割を果たす。デジタル認証システムを用いることで、ユーザーとサービスプロバイダー間で匿名性を保ちつつ認証と責任追跡が可能な取引を実現できる。また、プライバシーを保持する本人確認管理システムの構築にも活用される。[50]

エンドユーザー主導型・コミュニティ主導型の暗号化と共同サービス

インターネットの強みの一つは、エンドユーザーが関連するインターネットサービスプロバイダーと調整することなく、ネットワークのアプリケーションや利用方法を開発できる点にある。この特性に関連し、利用可能な暗号化ツールの多くは、従来のサービスプロバイダーや組織ではなく、フリー・ソフトウェアやインターネットエンジニアリングコミュニティの専門家によって開発・提供されている。これらの取り組みの主な焦点は、プライバシー強化テクノロジー（PET）を生み出すことにある。これは、サービスプロバイダーとのやり取りにおいて自らのプライバシー利益を守ろうとする意思と能力を持つ、関心のある（そしておそらく技術的に有能な）ユーザーが、単独または共同で導入できるものである。

こうしたPETには、スタンドアロンの暗号化アプリケーションや、ウェブ通信の機密性を維持したりオンラインサービスへの匿名アクセスを可能にするブラウザ拡張機能が含まれる。電子メール用暗号化技術であるPGP（プリティ・グッド・プライバシー）は、この種のテクノロジーで最もよく知られ、最も初期の事例の一つだ。ユーザーはメールリーダーに加えて、コンピューターに追加ソフトウェアをインストールすることでPGPを利用できる。このカテゴリーのテクノロジーは、中央集権的なサービスプロバイダーに依存せずに、エンド・ツー・エンド暗号化やその他の保護機能を提供するように設計されている。特に、PGPを基盤とするGnuPGソフトウェアのようなクライアントサイドソリューションは、送信者と受信者が、ブロードバンドプロバイダー、ソーシャルネットワーク、ウェブメールサービスといった信頼できない、場合によっては敵対的な仲介業者を、暗号化サービスを実現するために依存することなく利用できるように設計されている。メール以外の通信例もある。Scramble! や Cryptogram はソーシャルネットワーク向けプラグインの例であり、ユーザーにエンドツーエンドの暗号化を提供する。

48 ブルース・シュナイアー.『私たちインターネットの巨人たちに魂を売り渡した—それ以上を』. 2015年5月. https://www.schneier.com/essays/archives/2015/05/how_we_sold_our_soul.html.

49 Gürses と Preneel による同上。

50 クラウディア・ディアス、オマー・テネ、セダ・ギュルセス『英雄か悪党か：プライバシー法とテクノロジーにおけるデータ管理者』オハイオ州立大学法学ジャーナル第74巻923頁、2013年。

通信の暗号化である。[51] 一方、キーストロークロガーのようなテクノロジーは、暗号化が適用される前に入力された内容を傍受できるため、保護を提供するには不十分である。情報システムやデバイスにハッキングして、復号化の瞬間またはその後でデータにアクセスすることも、同様の効果をもたらす可能性がある。

ユーザー向けの別のツール群は、ユーザーがインストール可能なインスタントメッセージング用ツールである。これらのツールは、いわゆるオフ・ザ・レコード（OTR）暗号化プロトコルを統合し、通信の機密性、*完全な前方秘匿性*、*否認性*を提供する。完全な前方秘匿性は、暗号化鍵が侵害された場合に漏洩する通信量を最小限に抑える。これは、通信の機密性が単一の鍵の秘密性に依存せず、使用後に破棄される複数のセッション鍵に依存するよう設計されているためである。否認可能性とは、通信が終了した後は、チャット会話に関与したユーザー自身を含め、誰も技術的手段を用いて特定のユーザーが実際に特定のメッセージを送信したかどうかを技術的に証明できないことを保証するものである。これらの異なる特性は、口頭での会話に似たオンラインチャットサービスを実現するために設計されている。内容を隠蔽することで、サービスプロバイダー、接続事業者、政府が通信内容を根拠にユーザーの通信を検閲し、言論の自由を制限する能力も弱める。例えばFacebookチャットでOTRを使用すれば、市民ジャーナリストは特定の国に固有の制限的な利用規約や関連するコンテンツ削除慣行の適用を受けずに情報を伝達できる可能性がある。

特定のPETは、サービスを実現するために異なる当事者間の協力が必要だ。例えば、The Onion Router（Tor）[53]のような匿名通信システムは、システムユーザーが互いにカバーを提供するために参加し、それによって匿名性を実現するという核心的な考えに基づいて構築されている。[54] このようなシステムでトラフィックデータを記録・分析する政府や悪意のある主体は、匿名性集合内のどのユーザーが特定の行動に関連しているかを特定できず、ユーザー間の通信パターン（すなわち通信グラフ）を復元することもできない。[55] 以下の小節では、このようなメタデータの保護についてさらに詳しく論じる。

前述の様々なPETはサービスプロバイダーによる実装を必要としない。ただし、サービスプロバイダーが相互運用性を提供したり、こうしたテクノロジーの使用をブロックしたりすることで、その利用を促進・抑制することは知られている。例えば、サービスプロバイダーは特別な.onionアドレス経由でのアクセスを提供することで、匿名ブラウジングソフト利用者と相互運用性を高められる。[56] これによりユーザーのセキュリティが向上する。

マルチパーティ計算（MPC）技術は、機密データを保有する複数のNGOなど、関係者が互いのデータセットを明かさずにデータ分析を可能にする協調的解決策のもう一つの例である。これらの設計には共通点があり、信頼できる中央集権的権威が存在しない状況下でも、暗号化を活用してプライバシーとセキュリティの保証を提供するという点である。

---

51 http://cryptogram.prglab.org (最終アクセス日: 2016年8月29日)。

52 https://otr.cypherpunks.ca (最終アクセス日: 2016年8月29日)。

53 https://www.torproject.org (最終アクセス日: 2016年8月29日)。

54 匿名性に関する技術用語の議論については、Pfitzmann and Hansen, 2005 を参照せよ。

55 Diaz、Tene、Gürses、前掲書。

56 Tom Fox-Brewster. Facebook opens up to anonymous Tor users with onion address. The Guardian. 2014年10月31日. http://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users-onion（最終アクセス日：2016年8月29日）。

最後に、金融取引への暗号化のアプリケーションについて言及する価値がある。いわゆるブロックチェーンプロトコルを用いた暗号通貨の実装には、近年多くの進展が見られる。これらのシステムには多くの利点があり、またこれらのプロトコルは、新たな形態の契約や電子認証にも有用であり、法的インフラが容易に入手できない状況下では有用な補助手段となり得る。支払いに関連するプライバシー保護について言えば、ビットコインで使用される暗号技術が匿名支払いを保証するという誤解が一般的である。しかし技術的には、ビットコインが提供する唯一の保護は擬似匿名性である。[57]

メタデータの暗号的保護

メタデータ、すなわちユーザーの通信行動に関する情報の入手可能性は、ユーザーにとって特に脅威となり得る。ここで言うメタデータとは、サービスプロバイダーがサービス提供を通じて観察可能な情報を指す：ユーザーがいつ、どの頻度で、どの程度の時間、誰と通信しているかといった情報である。こうしたデータから通信グラフや詳細な行動パターンを推測することが可能だ。[58] メタデータは地理的な追跡にも利用され、人々を匿名通信から妨げとなる。バークマン・センターの報告書が指摘するように、メタデータは通常、政府がアクセスできない形で暗号化されておらず、したがって「インターネット通信テクノロジーが普及する以前には得られなかった膨大な監視データを提供する」[59]

前セクションで論じたツールや解決策だけでは、サービスプロバイダーによるトラフィック分析からメタデータを保護することはできない。したがってエンド・ツー・エンド暗号化メッセージングサービスを利用しても、ユーザーは通信内容自体は保護できるが、通信メタデータ（通信が行われた日時や相手先）はサービスプロバイダーに提供されることになる。通信が暗号化され認証されていても、様々な接続プロバイダーやサービスプロバイダーが、こうした暗号化された通信を監視できる立場にある可能性がある。意味のあるメタデータの露出を最小限に抑えるためには、暗号化ツールと通信の匿名性を提供するテクノロジーを組み合わせて使用する必要があるかもしれない。

オニオン・ルーター（通称Tor）は、ウェブサイトやオンラインサービスに匿名でアクセスする機能を提供する。Torは、ユーザーとウェブサイトとの通信を中継する仲介業者を運営するボランティアコミュニティの要件を必要とする。これにより第三者がユーザーの通信相手を監視できなくなる。暗号化技術を用いることで、各プロキシは通信経路の一部しか認識せず、単独のプロキシではユーザーと訪問先ウェブサイトの両方を特定できない仕組みだ。サービスプロバイダーの視点では、Torはクライアントサイドツールと見なせる。個人がサービス側を変更せずに単独で利用できるからだ。前述の通り、サービスプロバイダーは特別な.onionアドレスで私たちのウェブサイトへのアクセスを開放することで、Torとの相互運用性を高められる。

ユーザーがTor経由でウェブサイトにアクセスする場合、サービスプロバイダーはユーザーの身元を特定できない。ユーザーの身元は一連のプロキシによって隠蔽されるからだ。さらに、ウェブサイトが異なるセッションを単一のユーザーに紐付けることも不可能であり、事実上あらゆる追跡を無効化する。

---

57 参照：Bitcoin is NOT anonymous, http://www.bitcoinisnotanonymous.com/ (最終アクセス日：2016年9月14日)

58 例：Tokmetzis, D.「無邪気なスマートフォンが、あなたのほぼ全人生を秘密のサービスに漏らす仕組み」、2014年。英語訳は https://www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/ (最終アクセス日: 2016年5月15日) に掲載されている。

59 バークマン・センター 2016年。

追跡能力。もちろん、Torはユーザーがサービスプロバイダーに直接身元を明かす場合、そのサービスプロバイダーに対する匿名性は保護しない。

匿名性の保護に加え、TorはユーザーのISPがコンテンツへのアクセスをブロックしている場合にも有用だ。ユーザーはTorを利用してブロックされたウェブサイトにアクセスできる：ユーザーのISPはユーザーがTorプロキシの一つに接続していることを観察できるが、ユーザーが実際に通信しているウェブサイトを見たりブロックしたりすることはできない。これはVPNが提供できる保護と類似している。一方で、ウェブサイトなどのサービスプロバイダーは、Torネットワークからの接続をブロックできる。悪意のあるトラフィックがTorトラフィックとして到達する可能性や、Torトラフィックがビジネスモデルを妨害する可能性があるため、サービスプロバイダーはそうした措置を取る動機を持つ。この妨害は、ユーザーがオンライン上の匿名性を保護する最も効果的な手段を利用できなくする恐れがある。

Torブラウザは、ユーザーがインターネット上で通信する際、通信の起点と終点を難読化することを可能にする。ここで*言う難読化*とは、ユーザーの実際のオンライン活動と見分けがつかない「偽の」信号を自動生成し、ノイズの多い「覆い」を提供することで、ユーザーの実情報と通信行動を観察不能に保つことを指す。近年、オンライン上のユーザー保護手法としてオブラフスケーションが注目されている。([60]TrackMeNotは検索エンジンユーザー向けのオブラフスケーションツールである：このプラグインは検索エンジンに偽の検索クエリを送信し、検索エンジン提供者がユーザーの正確なプロファイルを構築する能力を阻害する。TrackMeNotやその他の検索オブラスケーションツールは、検索エンジンがユーザー生成クエリとコンピュータ生成クエリを区別できる特定の攻撃に対して脆弱であることが判明しているが、検索や位置情報サービスのように情報開示が避けられない場合、オブラスケーション技術のさらなる進歩はユーザー保護に肯定的な役割を果たす可能性が高い。メタデータの普及と、メタデータを用いて人々やユーザー行動を推測する可能性を考慮すると、デジタル環境におけるユーザー保護のため、暗号化と難読化手法の連携強化に関する研究開発が進むだろう。

3. 暗号技術、法、人権：背景

本セクションでは、現行の国際法とポリシーが、暗号化テクノロジー、その入手可能性、およびサービスやユーザーによる導入とどのように関連しているかについて簡潔に概説する。まず、暗号化が政府による情報・通信への合法的アクセスを阻害する障壁として位置付けられるという顕著な議論に言及する。この主張、すなわち暗号化が政府関係機関による進行中の捜査に関連する情報・通信への合法的アクセスを妨げるという主張は、悪意ある行為者の通信・情報行動が「闇に沈む」現象として要約される。

続いて、一般的な電子商取引、データ保護、セキュリティポリシーにおける暗号化規制の位置付け、および暗号化が標準化団体や枠組みにおける議題である事実について簡潔に説明する。これにより、規制が実際にもたらすべき大きな枠組みが明らかになる。すなわち、規制は概して暗号化の促進・採用・展開を中核的関心事とすべきであり、その活用を通じてセキュリティとプライバシーの保護、グローバルな商取引の実現、政府業務の安全確保、そしてデジタル環境全体における信頼の構築を促進する手段として機能するのだ。

60 参照：Brunton, Finn, and Helen Nissenbaum. *『オブリュスケーション：プライバシーと抗議のためのユーザーのガイド』* MIT Press, 2015.

本セクションは、暗号化に関する国際規範と、プライバシー及び表現の自由という人権保護における暗号化の支援的役割への最近の注目について、簡潔に論じて締めくくる。

「暗闇化」か「監視の黄金時代」か

強力な暗号化の一般利用に制限が必要かどうかという疑問を最も端的に提起しているのは、暗号化と、それが政府による情報・通信への合法的アクセスに与える影響に関する議論である。これは、犯罪の捜査や国家安全保障の保護において、暗号化が障害となり得る可能性があるためだ。例えば、特定の捜査における証拠の相当な理由を確立する裁判所承認令状など、情報・通信へのアクセスを得るための手続き上・実質上のあらゆる保護措置が講じられた場合であっても、暗号化によって効果的なアクセスが阻害される可能性があるという考えは、公共の安全と国家安全保障への影響について一貫して懸念を引き起こしてきた。これは1990年代の強固な暗号手法の一般公開をめぐる最初の議論でも問題となり、現在も同様である。この状況は政府高官らに、容認できない事態であるとの声明を発表させるに至った。そして、アクセスへの障壁となり悪意ある活動の闇化を招くという理由で強力な暗号化を制限する提案が相次いだり、関連当局向けの何らかの例外的なアクセス権を確立しようとする動きにつながったのである。[61] 最近のテロ事件は暗号化制限のさらなる要求を招いた一方で、[62] ドイツやオランダなどの一部の国々はインターネット上の暗号化制限に強く反対する立場を取っている。[63] 欧州ネットワーク情報セキュリティ機関（ENISA）とユーロポールも共同声明で、暗号化製品へのバックドア導入に反対する立場を示している。[64] 最近ではフランスとドイツの内相が共同で、特に外国の管轄区域から提供されるエンド・ツー・エンド暗号化によって法執行機関が直面する課題への解決策を模索する必要性を表明した。[65]

この議論を完全に扱う場ではないが、本調査の目的上、技術コミュニティにおいて圧倒的な合意が存在する点を明確にしておく必要がある。すなわち、適切に実装された暗号手法が確立し得るセキュリティの観点から、関連政府機関による例外的なアクセスには根本的な欠点が付随するという点である。[66] 多くの提案が技術的に実現不可能であるか、効果的に施行できないという事実に加え、それらは意図しない主体への脆弱性を生み出し、すべての者のセキュリティを低下させる。そして最終的な目標を達成できないだろう。[67] 私たちはさらに、制限はサイバーセキュリティ、貿易、電子商取引に深刻な悪影響を及ぼす。[68]

---

61 参考文献参照。

62 Berkman 2016.

63 McCarthy 2016。ドイツに関する議論についてはセクション4を参照。

64 ENISA および ユーロポール。21 世紀のデータ保護を尊重する合法的な犯罪捜査について。ユーロポール および ENISA 共同声明。2016年 5 月 20 日。

65 Cazeneuve 2016。

66 例えば、ハロルド・アベルソンら『ドアマットの下の鍵：政府による全データ・通信へのアクセス要件がもたらす不安定性』2015年7月。http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf。

67 ブルース・シュナイアー。前掲書。

68 スワイア。シカゴ・トリビューン紙も参照。暗号化とテロリストの足跡、http://www.chicagotribune.com/news/opinion/editorials/ct-fbi-terror-encrypt-apple-Google-edit-1214-20151211-story.html （最終アクセス日：2016年8月29日）。ニコラス・ウィーバー。私たち暗号化がテロリストの隠れ蓑になると考えている。そうではない。2015年12月。https://www.washingtonpost.com/news/in-theory/wp/2015/12/14/we-think-encryption-allows-terrorists-to-hide-it-doesnt。

したがって、暗号化の導入が、保護されたデータや通信へのアクセスを求める法執行当局やその他の機関に与える課題は、容易な解決策のないまま課題として残っている。[69] *暗号化によって*、犯罪防止、公共の安全、国家安全保障の目的で、政府が情報と通信への十分な法的アクセスを確保するという点において、法執行機関にとって実際の問題がどれほど大きいかという疑問は、軽視できない。私たち議会の公聴会で証言した専門家ピーター・スワイアは、政府が直面する現状を「監視の黄金時代」と表現した。[70] 有名な法律実務家クリストファー・クーナーは、1990年代の暗号化と政府の合法的アクセスを巡る第一の議論を振り返り、暗号化推進派がその議論に勝利したという一般的な認識について、実際には誤りだったと述べている。[71] ハーバード大学バークマン・センター・フォー・インターネット・アンド・ソサエティもまた、「暗闇に陥る」と特徴づけられる状況は存在しないと結論づけている。[72] 同センターはこう論じる：「テクノロジーの開発の軌跡は、暗号化されていないデータが豊かに存在する未来を指し示している。その一部は、法執行機関が『暗闇に陥る』と恐れる通信経路の空白を埋めるだけでなく、それを超える可能性すら秘めている。」[73]

要約すると、公共の安全を理由に強力な暗号化の自由な展開を妨害する提案は数多く存在するが、その妥当性を評価すると、これらの提案は厳密な科学的検証に耐えられない。さらに、これらの提案は、ユーザーにとって何が危機に晒されているかというより根本的な問題を回避している。デジタル通信やコンピューティングのユーザーが直面する既存の脅威環境を考慮すれば、より高度なセキュリティ対策は正当化され、必要である。これは特に、通信の機密性に関して特別なニーズを持つユーザーに当てはまる。国家・非国家アクターからなる国際的な広範な集団を含むこの脅威環境は、ユーザーの情報と通信の保護を強化するサービスやツールにおいて、ユーザーの利益のために強力な暗号化がサービスで採択される傾向を後押ししている。[74] このようなセキュリティ強化の進展を逆行させることは、重大な後退となるだろう。

暗号化と法：広範な状況

暗号プロトコルの展開、使用、開発と法が関連する多様な側面のすべてを概観することは、本研究の範囲を超える。それでも、一般的な状況を概説するためには、そのアプリケーションの広大さを認識することが重要である。

人権保護と強く関連するのは、プライバシーとデータ保護に関する立法である。データ保護法を制定している国の数は現在、さらに

---

69 組織犯罪の文脈における課題に関する議論については、例えばユーロポール 2015（特に付録1：暗号化に関する議論）を参照のこと。

70 ピーター・スワイア証言 。上院司法委員会公聴会「暗闇へ：暗号化、テクノロジー、公共の安全とプライバシーの均衡」。2015年7月8日。ピーター・スワイア『暗号化とグローバル化』も参照のこと。コロンビア科学テクノロジー法レビュー、第23巻、2012年。http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602。

71 クナー 2013年。

72 バークマン・センター 2016年。

73 同上。

74 欧州議会向けの以下のテクノロジー評価も参照のこと。これは、政府による監視が個人に与える不均衡な脅威に対処するための様々なポリシーオプションについて議論し、リストアップしている。http://www.stoa.europarl.europa.eu/stoa/webdav/site/cms/shared/2_events/workshops/2015/20151208/ EPRS_STU(2015)527410_REV1_EN.pdf (最終アクセス日: 2016年9月14日)。

100を超える。[75] このようなデータ保護法によって規制される個人情報の公正かつ合法的な処理に関する主要な原則の一つは、セキュリティの原則である。この原則は、意図された受信者以外の者による違法なアクセスから個人データを保護するために、適切なセキュリティ対策が講じられることを意味する。2016年に採択するために採用され、2018年に発効する新しい欧州連合一般データ保護規則は、個人データのセキュリティに関して先進的な一連のルールを含んでいる。暗号化は、何百万人もの人々に影響を及ぼし得る個人データ侵害に対する重要な防護策となり得る。さらに、暗号化はプライバシーとデータ保護を設計段階で組み込む「プライバシー・バイ・デザイン」及び「データ保護・バイ・デザイン」の実現において特に重要である。21世紀のプライバシー保護とデータ保護の基盤としてますます受け入れられているこれらの原則は、暗号技術の革新と実装を通じてのみ実現可能である。

暗号技術はまた、インターネット上での電子商取引（e-Commerce）の条件を整える上で絶対に不可欠な要素であった。後述するOECD原則は、各国の暗号ポリシーがこれに干渉しないことを保証し、電子商取引の国際的発展の条件も確保するために採択するために採用された。

電子商取引とデータ保護に関する包括的なポリシー目標は、オンライン環境における信頼の促進である。人権の観点から、信頼の促進自体が目的であってはならないことに留意すべきだ。結局のところ、ここで最も重要なのは、人々が信頼を持つことではなく、自律性と人間の尊厳に関して実際に存在するリスクや危害に正当に対応する措置についての知識基盤が存在することである。([76]

国際暗号ポリシーと人権

暗号化に関するポリシー論議は、通信ネットワークやインターネットの国際的性質、貿易・グローバル化・国家安全保障の側面から、重要な国際的次元を持つ。実際、国際貿易とネットワーク化された通信は、国際的次元と国家的次元を切り離すことを極めて困難にしており、暗号化ポリシーの規範はオンライン環境において持続可能であるために国際的に合意される必要がある。この点を認識し、国際機関はデータ保護、経済政策、輸出管理、インターネットガバナンスの分野で、また最近では人権保護における暗号化の支援的役割に関して、暗号化関連の国際規範の策定に貢献してきた。IETF、W3C、インターネット協会を含む技術的なインターネットコミュニティも、政策声明や標準を通じて、暗号化政策に関連する国際的な進展に長年重要な貢献をしてきた。

OECDの「暗号ポリシーに関するガイドラインに関する勧告」は1997年3月27日に採択するために採用された。OECDは、採択後のレビューにより、同ガイドラインが策定された課題とポリシーに対処する上で引き続き適切であると結論づけられていると述べている。[77]このOECDのポリシー介入は主に加盟国を対象としており、3つの構成要素からなる。すなわち、OECD理事会の勧告、暗号政策ガイドライン（勧告の付属文書）、そしてガイドラインの背景と暗号政策に関する問題点を説明する「暗号政策の背景と問題点に関する報告書」である。

75 Greenleaf 2015。この集計では、セキュリティに関するルールが基準となった。
76 ケイが報告しているように、「オンライン上のセキュリティとプライバシーに関する傾向は深刻な懸念材料である」。前掲書 p. 12。
77 OECDガイドライン。

OECDの主な動機は、加盟国による商業分野での暗号技術利用に関するポリシー決定が「国内および国際的な情報通信ネットワークの発展を阻害する障壁」を生み出し、「国際貿易の発展を妨げる」可能性があったことである。

人権との関連性を最も明確に示している原則は、プライバシー及び個人データの保護に関する原則5である：

> 個人のプライバシーに関する基本的権利、すなわち通信の秘密及びあなたの個人データの保護は、国家の暗号政策ならびに暗号手法の実施及び利用において尊重されるべきである。

他の原則と同様に、説明が添えられている。そこにはこう記されている：「暗号化手法は、データ及び通信の機密性、個人の身元保護を含むプライバシー保護の貴重な手段となり得る。暗号化手法はまた、安全でありながら匿名の支払い、取引、相互作用を可能にすることで、あなたの個人データの収集を最小限に抑える新たな機会を提供する。」特に注目すべきは、この原則が電子取引の完全性を確保するための暗号技術利用に伴うプライバシー・データ保護上の課題を提起している点である。前述の通り、これには「個人データの収集や個人識別システムの構築」が含まれるため、必要に応じたプライバシー保護措置の確立が求められる。

OECDの「プライバシー保護及び個人データの越境流通に関するガイドライン」は、個人データの収集と管理に関する一般的な指針を提供しており、暗号化手法を実施する際には関連する国内法と併せて適用されるべきである。合法的なアクセスに関しては、原則は均衡のとれたアプローチを求めており、加盟国にかなりの解釈の余地を残している。

> 国家暗号化ポリシーは、暗号化データの平文または暗号鍵への合法的アクセスを認める場合がある。これらのポリシーは、ガイドラインに含まれる他の原則を可能な限り尊重しなければならない。[78]

原則の焦点は、貿易及び電子商取引の障壁の防止と促進に置かれている。この焦点を反映し、最も発展した原則は国際協力に関するものである。OECD原則は次のように述べている：

> この取り組みの一環として、政府は暗号ポリシーの名前のもとで、貿易に対する不当な障壁を除去するか、あるいはその創設を避けるべきである。

デイビッド・ケイが要約するように、デジタル時代の初期において「各国政府は、暗号化が世界経済の安全保障において果たす本質的な役割を認識し、政府発行の身分証明書番号、クレジットカードや銀行情報、企業の機密文書、さらにはオンライン犯罪そのものの捜査を保護するために、暗号化を利用またはその利用を奨励した」。メディア・通信環境における暗号技術の利用は他の分野に比べて発展が遅れており、メディア・通信のデジタル変革は比較的初期段階にある。

ユネスコは知識社会構想に関する研究において、関係者との協議を経て、暗号化をプライバシーと表現の自由に関するポリシーの関連要素と位置付けた。キーストーンズ報告書は「我々のデータが考慮される限りにおいて」と明記している。

---

78 この説明は次のように述べている：「この原則は、政府が合法的なアクセスを可能にする立法を制定すべきか否かを示唆するものと解釈されるべきではない」

私たち自身を代表するものである限り、暗号化は私たちのアイデンティティを保護し、ユーザーコンテンツの悪用を防ぐ役割を果たす。また通信内容（場合によってはメタデータも）が意図された受信者以外に閲覧されないことを保証することで、転送中のプライバシーと匿名性をある程度強化する。」[79]報告書は最終的に「匿名性と暗号化がプライバシー保護と表現の自由の促進手段として果たし得る役割」を認め、ユネスコがこれらの問題に関する対話を促進することを提案している。

市民社会主体が策定・採択するために定めた「必要かつ均衡の取れた原則」は、13の原則の一つとして通信システムの完全性保護を規定している。[80] ただし原則自体は` バックドアや暗号化導入制限といった具体的な暗号政策問題について明示的な指針を提供していない。

国連特別報告者デイヴィッド・ケイの最近の報告書は、暗号化と匿名性の人権状況に関する国連初の権威ある詳細な説明を提供している。[81] 報告書はまず、暗号化と匿名性ツールの現代的な状況について論じている。これらは、表現と意見の自由への入り口としてのプライバシー権、干渉を受けずに意見を持つ権利、表現の自由の権利に関連付けられている。報告書は暗号化と匿名性に対する様々な制限を評価し、実践におけるより良い保護、さらなる議論、関係者の行動への道筋を示す結論と提言を提供している。

ケイは例えば、暗号化がセキュリティを提供することで、個人が「自身の通信が意図した受信者だけに届き、干渉や改ざんを受けず、また受信する通信も同様に侵入から自由であることを確認できる」と指摘している（A/HRC/23/40 および Corr.1、パラグラフ 23 参照）。同報告書は、暗号化が情報へのアクセスに対する不当な制限を回避させ、表現の自由及び国境を越えた情報や思想へのアクセスを支持する仕組みであることを明確にしている。暗号化への干渉に対する法的枠組みの適用に関しては、この文脈における一般的な要件を概説し、以下のように述べている：

> […]比例性分析においては、暗号化と匿名性への侵害が、制限措置が抑止を目的とする犯罪・テロ組織ネットワークによって悪用される可能性が高いことを考慮しなければならない。いずれにせよ、表現の自由を侵害し得る制限措置に関する透明な公的議論を可能とするためには、「詳細かつ証拠に基づく公的な正当化」が不可欠である（A/69/397、パラグラフ12参照）。

報告書の主な結論は、「暗号化と匿名性、およびそれらを支えるセキュリティ概念は、デジタル時代における意見及び表現の自由の権利行使に必要なプライバシーと安全性を提供する」というものである。報告者は「こうした安全性は、経済的権利、プライバシー、適正手続き、平和的集会及び結社の自由、生命及び身体の安全に対する権利を含む他の権利の行使に不可欠である可能性がある」と確認している。制限の可能性を考慮し、報告書は「暗号化と匿名性への制限は、合法性、必要性、比例性、目的の正当性という原則に基づき厳格に制限されなければならない（A/69/397、パラグラフ56参照）」と述べている。具体的には、「裁判所命令による復号化は[…]、それが結果をもたらす場合にのみ許容され得る」と結論づけている。

---

79 ユネスコ『包摂的な知識社会を育むための基幹要素』パリ2015年

80 通信監視への人権適用に関する国際原則（「必要かつ比例原則」）。https://necessaryandproportionate.org で入手可能。

81 デイヴィッド・ケイ。意見及び表現の自由の権利の促進及び保護に関する特別報告者の報告書。2015 年 5 月。http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/ Documents/A.HRC.29.32_AEV.doc。

透明性があり公にアクセス可能な法律に基づき、個々の人物に対してのみ（つまり人々に対してではなく）、対象を絞った個別対応で適用され、司法令状の対象となり、個人の適正手続きの権利が保護される場合に限り、暗号化は認められる。

OECD原則及び国連暗号化問題特別報告者の最近の立場が示す指針は、人権保護における暗号化の重要性を明確に述べている。暗号化「バックドア」の義務付けが国際法と両立しないか否かのこの疑問に決定的な答えを与えるものではないが、その方向性を示唆している。一般的に、国際レベルで利用可能な指針は、暗号化に制限が課される場合、関連する人権が厳格に遵守されなければならないことを明確にしている。本報告書の第4セクションでいくつかの国別研究を選定した後、第5セクションでは、表現の自由とプライバシーに関する国際人権文書が暗号化の制限に適用されることについて、より深く議論する。

4. 選定国における国内レベルでの動向

文献を参考にすると、様々な法律やポリシーが暗号化の規制ガバナンスに影響を与える多くの方法が確認できる。本研究の目的範囲外ではあるが、関連する法律やポリシーにおける暗号化への制限や積極的措置の一般的な類型を概観することは有益である。その後、特定の国における事例研究をいくつか提示する。

一方で、暗号化には様々な制限が課される可能性がある。こうした制限は、個人や民間企業による安全な暗号化の使用を全面的に禁止したり、暗号化の使用を犯罪化したりするなど、非常に深刻かつ直接的な制限となる場合がある。また、特定の許可された主体や目的に対する登録要件、政府のライセンス要件、輸出管理するなどの条件となる場合もある。その他の関連制限には、迂回権限（例えば、発見されたが公表・修正されていないセキュリティ脆弱性の利用を通じたもの[83]）、暗号鍵開示権限、復号命令が含まれる。電子通信事業者に対し通信内容への合法的アクセス支援を義務付ける命令など、特定の復号命令は、事実上、サービスプロバイダーによるエンド・ツー・エンド暗号化の導入禁止に等しい。実際には、暗号化の利用には特定の問題のある法的仮定が伴う危険性がある。例えば、暗号化のユーザーは犯罪行為を隠蔽しているという仮定などである。最後に、法的制限以外でも、官民間の非公式な合意が、実際にはユーザーに対する安全な暗号化の制限につながる可能性がある。

一方で、既存の法律やポリシーには、様々な主体が暗号化対策の採択のために採用する積極的な措置が数多く含まれている。第3セクションで述べたように、データプライバシー法や電子商取引法は暗号化の導入を義務付け、奨励している。また、他の法律にも関連するセキュリティ要件が規定されている。さらに、標準設定に関する法律は暗号化標準の開発を促進し、業界全体で採択するために働きかけることができる。公共政策も、ユーザー教育プログラムやツール開発への財政支援を通じて、暗号化に積極的に貢献できる。

---

82 国連暗号化・匿名性に関する特別報告者報告書及びその基礎資料には、様々な制約と積極的措置に関する豊富な情報が含まれている。

83 こうしたセキュリティ上の脆弱性はゼロデイとも呼ばれる。

数学、コンピュータサイエンス、工学分野における暗号化関連研究の資金提供を通じても、暗号化に積極的に貢献できる。

以下では、暗号化政策に関する法的・政策的枠組みの国内状況について、5カ国の事例研究を検討する。ケーススタディは、制限と積極的措置について前述した一般的な類型に従っている。具体的には、ユーザーや組織によるメディア・通信環境での暗号化利用に関して、特定の制限が導入されているか、あるいは議論されているか、および／またはメディア・通信環境での暗号化の採択のために、積極的措置が取られているかを検証する。これらの研究は、国際的な観点から特に重要な国家レベルのポリシーの詳細について、より深く掘り下げている。本国別報告書で取り上げる国は、アメリカ合衆国、インド、ドイツ、ブラジルである。選定は地理的要因と関連資料の入手可能性に基づいた。アフリカ地域については、単一国における暗号化ポリシーの十分な特定情報源確保が困難な課題を克服するため、異なるアフリカ地域からの情報を提示する手法を採用した。これにより事例研究は五大陸を網羅する。各地域内の具体的な国も、暗号化ポリシー整備度合いに基づいて選定された。

アメリカ合衆国

アメリカでは1990年代以降、暗号化をめぐる広範かつ活発で論争的なポリシー議論が続いている。最初のポリシー議論と展開は「暗号戦争」と呼ばれ、1990年代に発生した。これには、通信事業者や機器メーカーに対し、効果的な盗聴の可能性を確保するよう求める要件を含む「法執行通信支援法（CALEA）」の採択のために年に採用した年に年に年に年に年に年に年に年に年に年に年この特定の事件は取り下げられ、強力な暗号化機能を備えたほとんどの商用製品に対する輸出管理の自由化と、これらの品目が国務省が管理する米国軍需品リスト（USML）から商務省が管理する商務管理リスト（CCL）へ移管された後、一般的な議論は解決した。[85] 米国商務省はCCL掲載品目に対し、登録義務、技術レビュー、報告義務などの管理を維持している。また、機密性の高い暗号化製品や外国政府への販売については、引き続きライセンスその他の要件を課している。

専門家間では、通信手段が電気通信からインターネットベースの通信サービスへ移行した結果生じたとされる「暗闇化（Going Dark）」問題に対処するための提案が継続的に行われている。この議論は近年顕著になり、大統領による数回の発言にまで発展している。現在の議論は、スノーデンによる暴露と、インターネットサービス、デバイスメーカー、ユーザーによる暗号化対策の配備増加が広く報告されたことを受け、技術コミュニティや市民社会から暗号化の利用とセキュリティ強化を求める協調的な要請がなされたことで再燃した。

84 Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010)

85 米国商務省『暗号化輸出管理：ライセンス例外ENC及び一般市場適格性の改訂』2010年6月参照。またIra Rubinstein及びMichael Hintze『暗号化ソフトウェアの輸出管理』http://encryption_policies.tripod.com/us/rubinstein_1200_software.htm（最終アクセス日：2016年9月14日）も参照。

大規模監視活動" [86] 産業界における暗号化の採用拡大は、特定の政府機関、特にFBIから批判的に受け止められている。これらは、法執行支援を目的としたiPhone情報へのアクセス可能性を巡る、AppleとFBIの広く報じられている法的紛争につながった。[87] 2016年には、米国法の下で暗号化に新たな制限を設ける複数の法案が米国議会に提出された。

概して、米国の法制度は、商業・貿易の安全性を確保するため、関連する状況において様々な暗号化手法を含むセキュリティ対策の実施を促進し、要件としている。こうした法律の概要は本国別報告書の範囲を超えるが、米国法には暗号化手法を促進・要件とする様々な法律が含まれている。関連法としては、2014年連邦情報セキュリティ近代化法（FISMA）、グラム・リーチ・ブライリー法、医療保険の携行性と責任に関する法律（HIPAA）、連邦取引委員会法が挙げられる。これらの法律はセキュリティ要件を規定しており、特定の状況下で暗号化の使用を間接的に要求または促進している。最後に、多くの州の個人情報漏洩通知法は、暗号化されたデータをセーフハーバーとして扱い、データを暗号化した企業を通知義務から免除している。

暗号手法の導入と利用に対する支援は国際的な文脈にも及んでおり、米国は国際協調の主要な推進国の一つである。米国政府は省庁の資金提供イニシアチブや国立科学財団を通じて、暗号手法と標準の研究開発を支援している。最後に、米国国務省民主主義・人権・労働局（DRL）は、インターネットの自由に関連する幅広いプロジェクトに資金を提供している。その目的は「オンライン上での基本的自由、人権、情報の自由な流通を促進すること」であり、これにはオンライン情報へのアクセス制限に対処するための強力な暗号化ソリューションへの政府資金提供も含まれる。([88]

米国における暗号化手法の法的扱いを巡る議論では、憲法上の考慮事項と人権が重要な役割を果たしている。暗号プロトコルの配布制限や暗号手法の公表制限は、表現の自由を保障する米国憲法修正第一条への干渉と見なされる。具体的には、第9巡回区控訴裁判所はソフトウェアのソースコードが修正第一条で保護される言論に該当し、その公表を妨げる政府規制は違憲であると判決した。[89] さらに、私たちの暗号化に関する法律とポリシーは、米国の競争力（米国に本拠を置く成功企業による海外での事業展開、インターネットサービス関連市場へのアクセスと優位性の確保）や、法執行機関、国家安全保障、情報機関による合法的な政府アクセス権益の考慮に強く影響されている。暗号化ポリシーに大きく関わる第三の要因は、米国の重要インフラを保護するという目的である。

---

86 Ira Rubinstein と Joris van Hoboken による『クラウドにおけるプライバシーとセキュリティ』（*Maine Law Review* 2014）を参照のこと。特に、暗号化に関する議論はスノーデン暴露以前から既に進行しており、米国の法執行機関はインターネットサービスへの盗聴義務（CALEA）の拡大を主張していた。議論については Adida ら 2013 を参照のこと。

87 エリック・ゲラー 2016年。

88 資金提供プロジェクトとプログラム効果の評価については、ライアン・ヘンリー、ステイシー・ペティジョン、エリン・ヨーク『国務省インターネット自由プログラムのポートフォリオ評価』を参照。ランド国立セキュリティリサーチ部門。2014年2月。http://www.rand.org/content/dam/rand/pubs/working_papers/ WR1000/WR1035/RAND_WR1035.pdf。より最近の研究では、こうしたプロジェクトが違法利用に悪用される疑問について評価している。Sasha Romanosky、Martin C. Libicki、Zev Winkelman、Olesya Tkacheva。インターネットの自由ソフトウェアと違法活動、犯罪者を支援することなく人権を支援する。ランド社。2015年。http://www.rand.org/pubs/research_reports/RR1151.html。

89 Bernstein 対 私たち司法省、第 9 巡回区。判決：1999 年 5 月 6 日。

米国には、暗号ポリシーと実践に関与する、特に活発で強力に発展した市民社会アクターがいる。同国は、暗号研究とエンジニアリング、暗号サービスの革新の開発と実装の主要拠点である。さらに、暗号化ポリシーに関する国内および国際的な議論に関与する、活気ある非政府組織（NGO）のコミュニティがある。[90]

強力な暗号化に対する主な干渉は、国家安全保障、法執行、外交の分野で発生しているか、検討されている。この領域において、また特定の通信への合法的アクセスを保証できるか否か、その方法に関する論争的な疑問に答えるにあたり、米国政府は国際的に自国のポリシーを次のように説明している。すなわち「責任ある暗号化技術の導入」が「私的通信や商業を含む日常生活の多くの側面を保護する」と同時に、「強力な暗号化へのコミットメントを弱めることなく、悪意ある行為者を責任追及可能とする」ことを目指すものであると。

この難しい均衡が米国で現在どのように実践されているかについて、以下の方法（暗号化の可能性のある情報や通信の領域外で十分な証拠が得られる可能性は別として）を通じて、いくつかの具体例が明らかになっている：

技術的支援規定

情報または通信への合法的アクセス条件が満たされた場合、米国法は他の法制度と同様に、関連サービスプロバイダーに対し、当局が求める関連情報・通信の提供を支援する法的義務を課す。前述の通り、CALEAは通信分野に対し、サービスプロバイダーが通信傍受を支援できる体制を確保するよう要件を定めている。電子通信プライバシー法は、サービスプロバイダー及び特定の他の事業体が「対象個人に提供しているサービスへの干渉を最小限に抑え、目立たない形で傍受を遂行するために必要な全ての情報、設備及び技術的支援」を提供することを要件としている。([91] 近年では、FBIがデバイスへのアクセス回避を目的とした裁判所命令の根拠として全令状法の適用範囲を模索している。AppleとFBIの間で広く報じられている法的紛争は、この新たな一連の事例の中で最もよく知られた例であるが、同様の要求が米国各地の異なる裁判所でも行われている。

非公式な協力

米国の法的枠組みは、政府による不当なアクセスからユーザーデータと通信を保護するための、様々な立法上・憲法上・規制上の保護措置を提供している。米国法は、企業と政府機関間の自発的な協力や非公式な合意のための法的余地を確かに設けており、刑事捜査や国家安全保障問題における最適な協力の確保も含まれる。ECPAは対象サービスに対する自発的開示に一定の制限を設けているが、それらは

90 例として「Encrypt all the Things」キャンペーンを参照のこと。

91 議論については[]を参照のこと。2008年FISAAAは、支援がユーザーに隠されたままであることを要求する、若干異なる文言を含んでいる。さらに、裁判所は全令状法の一般規定を用いて支援の要件を定めることができる。最近の事例に関する議論については、ジェニファー・グラニック『連邦判事が「暗闇化」論争にスポットライトを当てる』The Center for Internet and Society、2015年10月を参照のこと。http://cyberlaw.stanford.edu/blog/2015/10/federal-judge-shines-spotlight-%E2%80%9Cgoing-dark%E2%80%9D-debate (最終アクセス日: 2016年9月14日)。

データの提供を伴うものであり、そのようなデータを提供する能力に関する協力ではない。一般的に、米国の憲法上の保障は、要件である国家の行為が欠如しているため、自発的な協力のケースには適用されない。[92] 情報機関の上級職員は、政府の監視活動に関する最近の暴露がもたらした最大の影響の一つは、主要産業関係者が自発的な協力を継続する意思を次第に失っていることだと説明している。[93] 国際的に見ると、米国政府は他の国々と比べて特異な立場にある。なぜなら、国際的に最も成功しているインターネット企業の多くが米国に拠点を置いているからだ。

回避と保護の突破

最後に、保存または送信されるデータの暗号化は、適切に実装・運用されていても、ユーザーやサービスプロバイダーの関与なしに、情報通信への合法的アクセスを確保するため、関連当局によって回避または解読される可能性がある。例えば、関連当局はキーロガーのインストールやサイドチャネル攻撃などの手段を通じて、エンドユーザーデバイス上の非暗号化情報にアクセスできる。暗号化ソフトウェアや実装上の欠陥を悪用することも可能だ。ソフトウェアの脆弱性（いわゆる「ゼロデイ」）を修正せずに悪用する手法が、インターネットユーザー全体の不安定性を長期化させる点について活発な議論がある。最後に、上記選択肢の中で最も議論を呼んでいるのは、標準策定の文脈における暗号規格のセキュリティへの介入が記録されていることだ。これに対し技術コミュニティからは深刻な懸念が表明され[94]、国際的な専門家は関連する米国機関において攻撃的暗号関連能力と情報保証の分離が欠如している点を疑問視している[95]。具体的には、防御的セキュリティ確保の使命が、同じ機関内で攻撃的能力に注力する者たちによって損なわれる恐れがある。暗号化のセキュリティを回避または破るための様々な手法の使用に関する米国法上の法的規制と憲法上の審査は、まだ始まったばかりである。

これらの異なる選択肢とそれに関連する様々な課題を考慮すると、この点における米国の状況は依然として非常に流動的であり、法分野の幹部職員は

---

92 デレク・バンバウアー『オーウェルのアームチェア』シカゴ大学法学レビュー79号（2012年）、3頁、863-944頁を参照。https://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/uploads/79_3/01%20 Bambauer%20ART.pdf （最終アクセス日：2016年9月14日）。Solove 2002 も参照のこと。

93 ウィルソン・センター・シンポジウムを参照。私たちはどう変化したか？安全保障と自由に関する米国の見解の変遷。ボブ・リットの発言、https://www.youtube.com/watch?list=PLzM1iiQhVrdHHZPSZ1z_ztTrUuRPMUtRb&v=PWj8eqKKB64（「アメリカ人とアメリカ政府の間には、国家とその市民を保護するという利益のために、長年にわたる協力関係がある。[..] 企業に違法な行為をすることはなかった。企業には自社の弁護士がおり、自社の利益を守ることに長けている。しかし、NSAが埋めるべきテクノロジーギャップがあるように、法的ギャップも存在する。法律で明確に許可されていることと、法律で明確に禁止されていることの間には空間があり、その間にグレーゾーンが存在する。私たちはこのグレーゾーンにおいて、長年にわたり自発的な協力を得ることに非常に成功してきた。企業がこの種の
この種の自主的な協力が止まることは、国家を守る能力にとって疑いようのない損失だ」）。参照：マイケルズ、ジョン・D.、「大統領の諜報員たち：テロとの戦争における官民諜報パートナーシップ」（2008年10月6日）。カリフォルニア・ロー・レビュー、第96巻、901頁、2008年。SSRNで入手可能：http://ssrn.com/abstract=1279867。

94 エド・フェルテン。セキュリティのバックドアについて。Freedom to Tinker。2013年9月11日。https://freedom-to-tinker.com/blog/felten/on-security-backdoors/; ニール・コブリッツとアルフレッド・メネゼス。謎に包まれた謎。2015年12月。http://eprint.iacr.org/2015/1018.pdf; ダニエル・バーンスタイン、タンヤ・ランゲ、ルーベン・ニーダーハーゲン。デュアルEC：標準化されたバックドア。暗号学電子印刷アーカイブ：レポート2015/767。

95 アミール・ミズロック。監視とシリコンバレーが欧州のプライバシー均衡を「破壊」している。2015年12月11日。http://blogs.wsj.com/digits/2015/12/11/surveillance-silicon-valley-destroying-europes-privacy-balance。

法執行機関と情報機関は、暗号化されていない通信や情報へのアクセスを確保するための追加的な安全策を求めている。これらの提案は様々な形態をとっており、現在電気通信（携帯電話を含む）サービスにのみ適用されているCALEA要件のインターネットサービスへの拡大、鍵預託[96]、ゴールデンキー[97]の義務化、さらにはエンド・ツー・エンド暗号化機能の全面禁止などが含まれる。執筆時点では、ホワイトハウスの立場は新たな規制要件の導入にやや反対である。*ワシントン・ポスト紙*が公表したホワイトハウスのポリシー文書草案は、一般的に立法導入の拒否または延期を検討していることを明らかにしている[98] この文書はまた、法執行および国家安全保障の観点から、政府による合法的なアクセスを最適レベルで確保するための非公式な手段が依然として中心的な考慮事項であることを示している。

ドイツ

90年代後半の暗号化に関する国際的議論の一環として、ドイツでも通信暗号化への全面禁止の必要性と正当性について議論が行われた。その背景には、刑事捜査への影響があった。[99] 例えば英国とは異なり、同様の禁止措置はもはや真剣に検討されていない。[100] このような禁止措置の憲法上の正当性には深い疑念があり、また、その事実上の悪影響についても懸念がある。[101] 質的な観点から、暗号化に対する制限は、通信の秘密、人格権の一般的な権利の表現、そして間接的にはインターネット上で行使可能なあらゆるコミュニケーションの自由など、多くの基本的権利に影響を与えると考えられている。[102] このため連邦政府は1999年、暗号ポリシーの要点を定めた。これは暗号化を制限するのではなく、その安全性に信頼性を提供することを特に目的としている[103]

大まかに言えば、将来的な制限の可能性に関するドイツ内務大臣の発言は別として、ドイツは国連特別報告者デビッド・ケイの立場に同調し、制限しない、あるいは包括的に保護するポリシーを採択するために、個別の事例に基づいてのみ制限を採択する。[104] デビッド・ケイへの提出文書では、ドイツのサイバーセキュリティ戦略は、インターネット上における企業と個人の安全を確保することにあると明確にされている。連邦政府はしたがって、暗号化テクノロジーの利用を奨励し支援している。[105]

---

96 鍵預託制度とは、政府による合法的なアクセス要求時に利用可能とするため、暗号化鍵を第三者に保管させる要件を指す。

97 ゴールデンキーは、暗号化セキュリティへのバックドア設置を指す別称である。ゴールデンキー提案は、認可された当事者だけが鍵を知る安全なバックドアの構築を想定している。安全なゴールデンキーソリューションの実現可能性については、技術コミュニティ内で議論が分かれている。

98 暗号化に対する戦略的アプローチに関する国家安全保障会議（NSC）のオプション草案。2015年夏。http://apps.washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches-to-encryption/1742/。

99 アレクサンダー・コッホ。暗号化に関する基本権？CR 1997、106 ページ。

100 ゲリット・ホーヌング。暗号論争：アンデッドの復活。MMR 2015、145 以降。Kuner/Hladjk in Hoeren/Sieber。マルチメディア法。第 17 部、リサイタル 62 以降。

101 Koch 前掲書 p. 108 以降を参照。

102 ユリア・ゲルハルトス著『（基本）暗号化権？』（2010年）123頁以降を参照。

103 クナー／フラジク著『ホーレン／ジーバー編 マルチメディア法』第17部、64項。

104 David Kaye. 前掲書 § 57.

105 ドイツにおける暗号化テクノロジーの法的地位に関する国連特別報告者デイヴィッド・ケイへの提出文書。

これに関連し、治安機関向けのマスターキー（「バックドア」）が合理的かつ実現可能かどうかについて繰り返し議論がなされてきた。この議論では、暗号化アルゴリズム自体を対象とせず、むしろ「スニッファ」ソフトウェアや「キーロガー」を用いてパスワードや鍵を盗聴する方向性を持つ合法的アクセス制度について検討することで、より標的を絞った解決策の利用可能性と実現可能性も認識された。[106] 政府によるデータアクセス手段と、ドイツ基本法（憲法）に基づく必要な保護要件に関する判例は増加傾向にある。[107]

ドイツの人々は国際的に、プライバシー権と個人データ保護を特に重視する傾向があると評される。したがって、プライバシー保護と関連する安全策に対する人々一般の姿勢において、ドイツは特筆すべき存在と言える。BITKOMがドイツで実施した調査によれば、電子メールを暗号化する回答者の割合は2013年の6%から2014年には16%に増加した。1000人を対象としたこの調査は代表的とは言えないかもしれないが、暗号化利用の増加傾向は明らかだ。([108] ドイツでは複数のニッチな暗号化通信サービスや開発プロジェクトが活動している。例えばドイツ拠点のメールプロバイダーPosteoは、ユーザーデータの取り扱いにおいて新たな基準を確立しようとしている。([109]

例えばベルリンに本拠を置くインターネットメッセージングサービス「Telegram」は、ISISメンバーが利用しているとの噂が流れたことで最近話題となった。[110] ファイルやメールの暗号化ソフトウェア「Gpg4win（GNU Privacy Guard for Windows）」もドイツの開発者との関わりがある事例だ。スノーデン暴露事件の結果として、ドイツでは新世代のスタートアップが台頭したと言える。[111]

2015年11月、政府代表者と民間セクター代表者が共同で「信頼できる通信強化憲章」（Charta zur Stärkung der vertrauenswürdigen Kommunikation）に署名し、その中で「私たち世界一の暗号化拠点となることを目指す」と宣言した.[112] 欧州レベルや米国とは異なり、パリでの最近のテロ事件は暗号化に関する新たな国内議論を招かなかった。[113] ドイツ連邦情報セキュリティ庁は電子メール標準の実施に関する新たなガイドラインを提供し、安全な電子メールに関するIETFの新技術標準を支持した。[114] ドイツ政府は外交政策を通じて国際的なプライバシー保護を推進している。

---

106 ゲルハーズ。前掲書 p. 409。

107 判例に関する議論については後述を参照のこと。

108 BITKOM調査 2014年8月。サイバー犯罪。https://www.bitkom.org/Presse/Anhaenge-an-PIs/2014/ August/140827-BITKOM-Charts-PK-Cybercrime-mit-BKA-28-07-14.pdf。

109 マイケル・スカトゥーロ著『ドイツ流メール保護術』ガーディアン紙、2016年8月24日付、https://www.theguardian.com/technology/2014/aug/24/posteo-protect-email-the-german-way-patrik-lohr（最終アクセス日：2016年9月14日）。

110 マルクス・ベーム。メッセンジャー Telegram：ISテロリストのお気に入りアプリがプロパガンダチャンネルを閉鎖。2015年11月18日。http://www.spiegel.de/netzwelt/apps/is-auf-telegram-messenger-app-kuendigt-massnahmen-an-a-1063535.html。

111 イザベル・ド・ポムロー。スノーデンの後、暗号通貨スタートアップがドイツに根付く。2015年8月3日。http://www.csmonitor.com/World/Passcode/2015/0803/In-Snowden-s-wake-crypto-startups-take-root-in-Germany。

112 デジタルアジェンダ2014-2017、p. 33。

113 ファビアン・ヴァリスローナー参照。現場：暗号化。パリ事件後の責任問題。2015年11月19日。https:// netzpolitik.org/2015/tatort-verschluesselungstechnik-die-schuldfrage-nach-paris。ただし、ドイツ内務大臣とフランス内務大臣による最近の共同行動要請については、カズヌーヴ2016を参照のこと。

114 Richard Chirgwin, German infosec bureaucrats want mail providers to encrypt, The Register, 2015年10月21日, http://www.theregister.co.uk/2015/10/21/german_infosec_bureaucrats_want_mail_providers_to_encrypt/ (最終アクセス日: 2016年9月14日)

特にドイツはブラジルと共同で、人権理事会においてプライバシーに関する国連特別報告者の任命を約束した。[115]

政府が暗号化ポリシーを実施しようとする取り組みの例は複数存在する。非公式な行動から法律や規制に至るまで多岐にわたる。

ITセキュリティ法

2015年7月に施行されたITセキュリティ法（Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme）は、2011年に決定されたサイバーセキュリティ戦略に基づくものである。この法律は、特に重要なインフラ（例：通信分野）の事業者に、最低基準とITセキュリティインシデントの報告要件を通じて適切なネットワークセキュリティを提供する義務を課している。[116]

「De-Mail」法

暗号化技術を明示的に扱う法律のさらなる例として、いわゆる「De-Mail法」（*De-Mail Gesetz*）がある。この名前はドイツのトップレベルドメイン「.de」に由来すると見られる。同法の立法目的は、シグネチャー技術と暗号化技術を通じて信頼性と確実性を高めた新たな電子通信機能を確立することにあった。具体的には、民間事業者向けの新たなインターネット通信形態を規定・規制する内容も含まれる。[117] De-Mailサービスは提供に認証を必要とし、当局はの監督下にある（De-Mail法第17条〜21条）。De-Mail機能は、従来の電子メールとの互換性がないことも一因で、利用面では成功していない。また、エンド・ツー・エンド暗号化を実施していないため、セキュリティが最適ではないと批判されている。[118]

暗号化と情報セキュリティに関する業界固有の規制

ドイツでは暗号化と情報セキュリティに関して、いくつかの業種別ルールも存在する。例えば、電気通信法（TKG）には電気通信分野の基準が、エネルギー法（EnWG）にはエネルギー分野の基準が定められている。しかし欧州レベルでは、ネットワーク・情報セキュリティ指令（NIS指令）により、重要サービスプロバイダーおよびデジタルサービスプロバイダーは今後、より強固なセキュリティ対策が義務付けられることになる。[119]これに先立ち、国内レベルでは連邦情報セキュリティ庁法（BSIG）が既に改正されている。同法は「重要インフラ」（適用範囲についてはBSIG第8条c項参照）に対して共通の義務を規定している。

メディア教育上の警告と勧告

暗号化に関する情報を含むインターネットセキュリティは、メディア教育上の警告と勧告を通じて一般市民への教育の一環となっている。これらは

---

115 参照：Monika Ermert, NSA-Skandal:デジタル世界におけるデータ保護に関する国連特別報告者の設置を目指す、ハイゼ・オンライン、2015年3月23日、http://www.heise.de/newsticker/meldung/NSA-Skandal-UN-Sonderberichterstatter-fuer-Datenschutz-in-der-digitalen-Welt-angestrebt-2582480.html。

116 詳細については、Philipp Roos MMR の発表を参照のこと。Das IT-Sicherheitsgesetz、MMR 2015、p. 636。

117 実際の状況と歴史については、アレクサンダー・ロスナゲル著『Das De-Mail-Gesetz』を参照のこと。NJW 2011、1473 ページ以降。

118 参照：Andreas Voßhoff および Peter Büttgen。Verschlüsselung tut Not。ZRP 2014、p. 234。

119 https://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive を参照。

政府機関を通じて提供されている。例えば、連邦情報セキュリティ局（BSI）や州メディア当局は、ソーシャルメディアの賢明な利用についてアドバイスを行い、フィッシング詐欺、すなわち偽の電子メールメッセージを使ってインターネットユーザーに認証情報を入力させるよう仕向ける手口について警告している。例えば、ザールラント州メディア当局は、データを安全に暗号化するセミナーを開催している。[120]

ドイツにおけるITシステムの完全性に関する基本権利

憲法上の根拠に関して、2008年のドイツ連邦憲法裁判所によるオンライン検索に関する判決[121]及び情報自己決定権に関する判例は、暗号化技術の国際法上の取り扱いにおいて貴重な示唆を与える可能性がある。この判決の根拠となったのは、情報機関（ノルトライン＝ヴェストファーレン州憲法保護庁）が情報技術システムへの秘密アクセスを許可された授権規範であった。この規範は二つの要素から成り、インターネットの秘密監視その他の開示（選択肢1）と情報テクノロジーシステムへの秘密アクセス（選択肢2）を認めていた。裁判所はこれらの規定をドイツ憲法の下で精査し、本件の事実関係を超えた高い基準を潜入・操る行為に設定する機会と捉えた。

具体的には、裁判所はプライバシー権の一般原則に新たな次元を加えた。すなわち、*情報テクノロジーシステムの機密性及び完全性の保護を受ける権利*（いわゆる「IT基本権」）である。裁判所は、秘密潜入によるこの権利への干渉は、極めて重要な法的利益に対する具体的な危険の事実上の兆候が存在する場合にのみ許容されると結論付けた。潜入は原則として司法令状の対象となる。([122]) 裁判所が追求した保護の次元とテクノロジー進歩に伴う進展は広く確認され評価された。([123]) これは通信の秘密（進行中の通信のみを保護しシステム自体を保護しない）に対する適切な補完を構成する。

IT基本権において、憲法裁判所は比喩的に言えば、個人の人格の一部がITシステムに組み込まれるため、適用される保護もそれに伴って移行しなければならないと認めている。デジタル分野では、この考え方は1983年に情報への権利を確立した憲法裁判所の判決によって具体化されている。[124]

この新たな権利の具体的内容について、もう少し詳しく議論する価値がある。現代のデジタル環境において、保護される自己決定権は自己防衛の可能性を要件とする。この保護を達成する重要な手段は、デジタル環境における様々な暗号化の利用である。しかし、ITシステムへの侵入によって、この自己保護は回避される。これにより、個人は自らの管理する外のメカニズムやテクノロジーシステムへの依存度を高めることになる。

---

120 https://www.lmsaar.de/medienkompetenz/seminare/seminare-nach-themen-2/?mkz-action=details& seminarid=243.

121 BVerfG NJW 2008, 822.

122 BVerfG NJW 2008、822 (831 以降)。一部の法律評論家は、この表現は、既存の情報自己決定権に対する前進というよりも、それ自体が基本的権利を暗示していると批判している。マーティン・アイフェルト『インターネットにおける情報自己決定権。Das BVerfG und die Online-Durchsuchungen, NVwZ 2008, p. 521; Gabriele Britz, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, p. 441..

123 Thomas Böckenförde を参照。Auf dem Weg zur elektronischen Privatsphäre。JZ 2008、925 ページ以降。Gerrit Hornung。Ein neues Grundrecht。CR 2008、299 ページ以降。Thomas Stögmüller。Vertraulichkeit und Integrität informationstechnischer Systeme in Unternehmen。CR 2008, p. 435 et seq.

124 BVerfGE 65, 1; 例えば憲法におけるデータ保護の基盤。

憲法裁判所は、諜報機関によるアクセスに関してこれを確認している。これは特に、暗号化テクノロジーを回避し、それによって対象者またはそのサービスプロバイダーに対する望ましくないデータアクセスに対する自己保護規定を回避することを目的としている。同裁判所は、このような侵入を特に重い侵害と見なしている。[125] つまり、個人は基本的に、あなたの個人データの侵入や操る権利に対して自律的に防御する権利を認められたのである。要約すると、デジタル環境において、ドイツの情報自己決定権は、ITシステムに対する暗号化の使用権を意味すると言える。

しかし、別の疑問として、基本法自体に包括的に適用される「暗号化」が存在するか否かを問う必要がある。これは個々の権利の組み合わせから導出可能かもしれない。つまり、通信の秘密（基本法第10条第1項）と住居の不可侵性（基本法第13条第1項）も、特定の状況下では影響を受ける。技術中立的な通信の秘密により、現行の通信は政府による監視から保護されている。伝送中のデータの機密性を確保するため、この権利によって保護される暗号化の使用も考慮するのが論理的である。([126])

新たなIT基本権の文言には「保障」の要素が含まれる。これは判決が、政府の干渉に対する防御としての基本権の次元を超えていることを示している。裁判所によれば、国家は非国家アクターによる侵害から、個人が使用する情報テクノロジーシステムの完全性と信頼性を保護する責任も負う。

もう一つの憲法上の目的は、表現の自由の行使に対する「萎縮効果」を防ぐことだ。この負の効果は、1983年（国勢調査事件）に憲法裁判所が既に言及していた。[127]この点において、暗号化による事実上の保護と、例えば表現の自由の自由な行使のような個人の自由行使との間には関連性がある。したがって、ドイツ憲法のこのコンセプトにおいて真に自由と言えるのは、恐れを知らないコミュニケーションの自由の行使だけである。

さらに、判決の核心的な洞察は、現代のコミュニケーションが主にテクノロジーに依存している点にある。したがって、この分野における基本権利の効果的な保護には、テクノロジー通信インフラとその利用の保護も要件となる。[128] この客観的かつ機能的な人権保護アプローチは、ドイツ憲法法において強く発展している。技術的設計が言論の自由にとって重要であることは、国際的な議論においても認識されている。[129]

ドイツにおけるプライバシー・バイ・デザインとテクノロジーによるデータ保護の取り組み

複雑なITシステムにおける急速な発展に対して個人が無力であるという確認は、ドイツ法および国際法において適用される「テクノロジーと設計によるプライバシー保護」および「データ保護」というデータ保護概念にもつながっている。

125 BVerfG NJW 2008, 822 (830)。
126 Gerhards. 前掲書 p. 126 et seq.
127 BVerfGE 65, 1 (43)。
128 ヴォルフガング・ホフマン＝リーム『情報技術システムの機密性及び完全性の保障に関する基本権』JZ 2008年、1009頁以下。
129 参照：ジャック・バルキン『デジタル言論と民主主義文化：情報社会における表現の自由の理論』NYU Law Review 79 (2004)。

EUレベル。これらの原則の目的は、システム構想・設計の初期段階でプライバシー利益とデータ保護を積極的に考慮し、データセキュリティ法に関して頻繁に不可逆的な悪影響が生じるのを防ぐことにある。[130] プライバシー・バイ・デザインは、データセキュリティ、データ最小化、およびその保護能力の発展を支援する要素となり得る。

この重要性から、テクノロジーによるデータ保護とデータ保護に配慮したデフォルト設定は、欧州レベルで最近、一*般データ保護規則*（GDPR）を採択するために採用された重要な要素となっている。処理が法令の要件を満たし、かつ当該個人の保護を確保するためには、テクノロジー・組織的措置及び手順が必要である（GDPR第23条）。このアプローチは国内法においても、*連邦データ保護法*（Bundesdatenschutzgesetz, BDSG）第3a条及び第9条で示唆されている。第3a条はシステムデータ保護を、第9条はデータセキュリティを中核としている。[131] ドイツ国内法には革新的なアプローチが含まれているものの、それらはまだ成熟していない。例えば、第3a条の遵守不履行は、データ処理の実質的な違法性や制裁を自動的に招くものではない。[132]その結果、現時点でこれらのアプローチが実際にどれほど効果的であるかを評価することは難しい。

インド

インドの法律とポリシーは、銀行業務、電子商取引、機微な個人情報を扱う組織などにおいて、セキュリティ対策として強力な暗号化の実施を促進し要件としている。しかし、電子通信サービスによる暗号化の自由な導入には、いくつかの制限がある。具体的には、電気通信枠組みの下で規制されるサービスとのライセンス契約には、40ビットの暗号化レベルのみを許可する制限が含まれている（詳細は後述）。これらのサービスが強力な暗号化を導入する場合、政府による平文通信への合法的なアクセスを目的として、登録と鍵預託の慣行がある。これらのライセンス要件の正確な法的範囲、および対象サービスのエンドユーザーによる（サービスの利用または導入に対する）法的効力の程度については、顕著な法的不確かさが存在する。この法的不確かさは、インドにおける通信用の強力な暗号化の開発、導入、利用に悪影響を及ぼしているようだ：

> リスク回避的な企業は、暗号化レベルを40ビット以上には設定しない可能性がある。さもなければ、インド政府に「復号鍵」を開示し、事前の承認を求めるリスクを負うことになるからだ。[133]

暗号化に関する議論は、政府が暗号化使用に数々の制限を想定した草案を公表したことで、最近インドで公に再燃した。このポリシー[134]は、2008年インド情報技術（改正）法[135]第84Aセクションに基づき発出されたが、短命に終わった。しかし、プライバシー保護の安全策が欠如していることへの懸念は残っている。

---

130 参照：Voßhoff/Büttgen 前掲書 p. 232。

131 Ernestus in Simitis. Bundesdatenschutzgesetz. § 9 retical 1 et seq; Gola/Klug/Körffer in Gola/Schomerus. Bundesdatenschutzgesetz. § 9 retical 1 et seq; Jörg Pohle はこの主流の見解を批判している：Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens. FIfF-Kommunikation 2/15, 41 seq.

132 シュルツ前掲書 p. 208。

133 アパール・グプタ。何ビットで十分か？暗号化の合法性。2011年11月。http://www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/。

134 インド政府ポリシー草案。2015年9月。http://www.scribd.com/doc/282239916/DRAFT-NATIONAL-ENCRYPTION-POLICY（最終アクセス日：2016年9月14日）。

135 http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf（最終アクセス日：2016年9月14日）。

草案が示した表現の自由とプライバシーの権利を侵害する恐れがあった。[136]この抗議を受けて、インド政府はまず「現在ウェブアプリケーション、ソーシャルメディアサイト、Whatsapp、Facebook、Twitterなどのソーシャルメディアアプリケーションで使用されている大量利用暗号化製品」を適用除外とした。[137] その後まもなく、政府は提案されたポリシーを撤回し、新たなポリシーは未だ公表されていない。

2008年インド情報技術（改正）法第84Aセクションは、電子媒体の暗号化方式に関するルールを作成する政府の力をづける。同セクションは「中央政府は、電子媒体の安全な利用及び電子政府の推進のために、暗号化の方式又は方法を定めることができる」と規定する。この規定の文言は、ネットワークセキュリティの確保、電子商取引及び政府が使用することを促進する観点から、中央政府がルールを作成することを認めることを目的としていることを示唆している。ポリシー草案からは、インド政府が第84A条を、強力な暗号化の使用を要求・促進するのではなく制限する法的根拠と見なしているか、あるいは商業・私的領域における暗号化使用には政府認可が必要であるとの確認を示し、許可なき使用を全面禁止する姿勢を示しているように見える。

法律評論家らは、インド法、特に電子通信サービス分野において、どのような種類の暗号化の使用と導入が許可され、要件となっているかについて透明性が欠けていることを指摘している。[138]この法的不確かさの理由の一つは、電気通信法の分野に起因する。1885年インド電信法（及び改正法）は、電信の設置、維持及び運用に関する政府の排他的権限を広く規定しており、これがインドの通信サービスにおける主要な規制枠組みを構成している（第4セクション第1項）。同法第3セクション第1項は、「電信」という用語を広く定義し、以下を含むものと規定している。

> 電線、視覚的その他の電磁波放射、電波またはヘルツ波、ガルバニック、電気的または磁気的手段による、あらゆる性質の署名する、信号、文書、画像、音声または情報の伝送もしくは受信に使用される、または使用可能なあらゆる装置、器具、材料または機器を指す。[139]

したがって、理論上、インド中央政府は電子通信に対する広範な独占権を有しており、これにはインド国内における電気通信及びインターネットサービスの提供特権が含まれる。この規定は、1999年以降の電気通信自由化にもかかわらず、電気通信規制の対象となるサービスの提供には依然として適用される。[140] インド政府は、民間事業者との間でライセンス契約を締結することにより、関連する電気通信及びインターネットサービスの提供を民間事業者に認めている。これらのライセンス契約には暗号化の使用に関する規定が含まれている。[141] 具体的には、「インターネットサービス提供に関するライセンス契約」（第2.1条(vii)項）には次のように定められている：

---

136 Bhairav Acharya. インドの暗号化ポリシーの短命な冒険. 2015年12月. https://www.ocf.berkeley.edu/~bipla/the-short-lived-adventure-of-indias-encryption-policy/.

137 ナンダゴパル・ラジャン。暗号化ポリシー：抗議を受けてWhatsAppとウェブサービスが暗号化ポリシー草案から除外される。2015年9月。http://indianexpress.com/article/technology/tech-news-technology/draft-national-encryption-policy-you-might-need-to-store-whatsapp-messages-for-90-days/。（最終アクセス日：2016年9月14日最終アクセス）。Twitter上で、懸念するユーザーがハッシュタグ#ModiDontReadMyWhatsappを掲げて結束した。

138 アパール・グプタ。何ビットで十分か？暗号化の合法性。2011年11月。http://www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/。

139 『インド電気通信法・規制ハンドブック』2013年版。第1巻、179ページ。

140 参照：1999年インド国家通信ポリシー http://www.dot.gov.in/telecom-polices/new-telecom-ポリシー-1999; 及び2012年の最新版。http://www.dot.gov.in/sites/default/files/NTP-06.06.2012-final.pdf。

141 アパール・グプタ、前掲書。

(vii) ライセンシーは、ISPによるバルク暗号化が導入されないことを保証しなければならない。さらに、個人・当グループ・組織は、ライセンサーの許可を得ることなく、対称鍵アルゴリズムにおいて40ビット鍵長、または他のアルゴリズムにおける同等の鍵長までの暗号化を使用することが許可される。ただし、この制限を超える暗号化機器を導入する場合は、個人・団体・組織はライセンサーの事前の書面による許可を得るとともに、復号鍵を二分割してライセンサーに預託しなければならない。

一般的に許可されている（対称）暗号化の規定レベル（40ビット）は、安全でないと考えられる可能性がある。特に、40ビットレベルは、以前の私たち輸出管理下で許可されていた暗号化レベルに相当する。最近、ウェブサイトとの安全な通信実装にセキュリティ上の脆弱性が発見された。この脆弱性は、ユーザーとウェブサイト間の接続を強制的にこれらの旧輸出規制レベルまで暗号化を低下させる可能性を悪用するものであった。これは、セキュリティに対する制限の悪影響が、その法的有効期間をはるかに超えて長く続く可能性があることを示している。

さらに、より強力な暗号化の使用に関するライセンス契約の文言は、インドにおける鍵預託の実践を反映している。鍵預託制度は、後述するブラックベリーのインド事業をめぐる議論で広く取り上げられた事例によって具体化された。[142] 携帯電話サービスライセンス契約には、暗号化使用に関する同様の制限が含まれており、強力な暗号化を導入するエンドユーザーデバイスの検査と要件を義務付けている。[143] これらのライセンス条項はより制限的な環境を示唆しているが、民間企業は40ビットを超える強力な暗号化を実装している。

インド政府が公表した第84Aセクションに基づく暗号化ポリシーの草案は、2008年にこの規定を採択するために実施された協議プロセスを踏襲している。特に2009年には、インドデータセキュリティ評議会が暗号化ポリシーに関する勧告を発表した。[144]この勧告では、インドの法執行機関が暗号化されていないテキストにアクセスする必要性について詳細に論じられているが、人権に関する考慮事項は比較的未発達である。勧告は、利害関係について次のように述べている：

暗号化ポリシーには、様々な技術的問題、国家安全保障問題、企業のプライバシー、電子商取引や電子政府アプリケーションの成長に対する国際的な競争圧力などの考慮が必要である。グローバル化が進む経済環境において、インドの産業とビジネスの持続的な経済成長には、企業部門の従業員やビジネスパートナーを含む全ての正当なユーザーが暗号技術を利用できることが要件とされる。

これは、インドの国際的な経済競争力に関するポリシーにおいて強い配慮がなされていることを示している。具体的には、データセキュリティ評議会は「法執行機関が適正手続きや裁判所命令なしに平文開示を要求する場合、外国企業はインドへの業務委託を制限する可能性が高い」と指摘している。[145] この勧告は、暗号化のさらなる促進と自由化を提案し、登録要件の採択を否定するとともに、適正手続きの保障を遵守しつつ法執行機関による平文アクセスを一般的に確保する方法を規定している。

142 参照：Paul Taylor. Security that makes spies feel insecure. *Financial Times*. 2010年8月2日, http://www. ft.com/intl/cms/s/0/7ad48c10-9e5d-11df-a5a4-00144feab49a.html#axzz3R5nCIW6I.

143 アパール・グプタ。前掲書。

144 2008年IT（改正）法第84A条に基づく暗号化ポリシーに関する勧告を参照せよ。

145 2008年IT（改正）法第84A条に基づく暗号化ポリシーに関する勧告、p. 11。

インドの法制度における鍵預託とライセンス慣行、およびそれらが国際的に事業を展開する通信サービス企業とどのように関わるかの実例として、国際メディアで議論されたブラックベリーの事例がある。[146] インド政府はブラックベリーに対し、電子メールとSMSの監視を許可するよう要求した。[147] インド当局からの合法的なアクセス要件に対応するため、ブラックベリーはムンバイに国内事務所を設置した。正確な詳細は不明だが、このケースでは鍵がブラックベリー自身によってエスクロー保管されていたようだ。

金融サービスと取引の分野では、関係する利害関係者による暗号化の要件について特定の規制がある。インド準備銀行のガイドラインによれば、全ての銀行取引には最低128ビットSSL（Secure Socket Layers）暗号化が求められる。インド証券取引委員会（SEBI）は標準的なネットワークセキュリティとして64ビット/128ビット暗号化を規定し、データの安全性・信頼性・機密性確保のため暗号化テクノロジーの使用を義務付けている。([148] 2000年制定の「情報技術（ 認証機関）ルール」では、インド中央政府がデジタルシグネチャーおよび関連する公開鍵暗号規格のための暗号手法の枠組みを定めている。[149]また、IT法第43A条に基づく2011年情報テクノロジー（合理的なセキュリティ慣行・手順及び機微な個人データ・情報）ルールでは、生体認証、医療情報、性的指向、パスワードを含む機微情報に関して、商業主体による合理的なデータ保護・セキュリティ慣行の実施を要件としている。[150]

過去10年間、インドがデュアルユース物品の輸出管理を管理する目的でワッセナー・アレンジメントに加盟することに対し、国際的な支援が一部見られた。[151] インドの外国貿易に関する規制は、「情報セキュリティを含む情報テクノロジー」の輸出制限を規定しており、これには「暗号化プロセスを使用するデータ処理セキュリティ機器、データセキュリティ機器、伝送および信号伝送回線セキュリティ機器」が含まれる。[152] この表現は、ワッセナー・アレンジメントの軍需品リストで使用されている表現と全く同じである。[153] これらのルールについての解釈および実際の施行に関するデータはない。

146 議論については、Citizen Lab（トロント大学ムンク国際問題大学院）およびコリン・アンダーソン著「表現の自由の権利を確保するためのデジタルセキュリティソリューションの民主化の必要性」も参照のこと。2015年2月10日。http://www.ohchr.org/Documents/Issues/Opinion/Communications/CitizenLab.pdf。

147 A. Parvathy、Ravi Shankar Choudhary、Vrijendra Singh。インドにおける暗号に関する法的問題。2013年4月。*International Journal of Computer Application*、第3号、第2巻、http://rspublication.com/ijca/april13/6.pdf。Citizen Lab および Collin Anderson 2015 も参照のこと。

148 セクション 3(a) および参照 DOT ポリシー、http://www.nseindia.com/invest/resources/download/sebi_ circ_27082010.pdf。

149 2000 年情報テクノロジー（認証当局は）ルール、http://cca.gov.in/cca/sites/default/files/files/ rules.pdf（最終アクセス日：2016 年 9 月 14 日）。

150 通信情報テクノロジー省、通知、ニューデリー、2011年4月11日、http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf （最終アクセス日：2016年9月14日）。

151 通常兵器及び両用物品・テクノロジーを管理する輸出管理に関するワッセナー・アレンジメント。インドの加盟支援については http://www.nti.org/treaties-and-regimes/wassenaar-arrangement/を参照。

152 商工省、通知第14号（RE-05）/ 2004-2009、ニューデリー；2005年7月15日、http://www.vertic.org/media/National%20Legislation/India/IN_Amendment_of_ITC_HS_Export_and_Import_Classification_2005.pdf（最終アクセス日：2016年9月14日）で閲覧可能。

153 http://www.wassenaar.org/wp-content/uploads/2015/06/WA-LIST-13-1.pdf。

ブラジル

スノーデン事件の暴露後、ブラジルは国連においてプライバシー権を推進し、米国の大量監視を非難する国際連合の最前線に立った。最近の動向では、暗号化技術の利用と導入に関して、ブラジルは多様な目的を示している。一方で、同国はインターネットに関する法的枠組みの整備において主導的役割を果たしている。他方で、暗号化テクノロジーの普及を制限する可能性がある複数の措置を講じている。

現時点で、ブラジルではソフトウェア・ハードウェアを問わず、暗号化テクノロジーに対する輸出入の管理は存在しない。暗号テクノロジーの使用についても管理するものは存在しない。2015年、公の意見聴取と議論を経たプロセスで、ブラジル議会は新たな個人情報保護法案（「proteção de dados pessoais」）を起草した[154]。これは2016年5月13日に連邦議会に提出され、2016年法案第5276号として施行された。この法律は、オンライン上の慣行を含む個人データとプライバシーを規制・保護し、個人データの取り扱いにおける暗号化などのより安全な手法に関する規定を含んでいる。また、セキュリティ問題や、企業による攻撃やセキュリティ侵害の報告義務についても規定している。第44条(III)では次のように述べている：

> *管理者は、データ主体に被害を与える可能性のあるセキュリティインシデントを直ちに管轄機関に報告しなければならない。*
>
> *通知には少なくとも以下を含めること：[...]*
>
> *III – データの保護のために私たちが使用するセキュリティ対策の詳細、暗号化手順を含む；*[155]

それ以外には、法案に暗号化に関する規定は含まれていない。

執筆時点では、政府の一部だけでなく軍や司法機関も巻き込んだ複数の汚職事件が発覚したことで引き起こされた政府危機と全国的な抗議活動が、市民社会に法の支配の弱体化に対する新たな懸念を抱かせている。こうした動きが暗号化を含む情報通信ポリシーに広範な影響を与えるかどうかは、今後の見通し次第である。

マルコ・シビル

マルコ・シビル（ブラジル版インターネット権利法）により、ブラジルはインターネットに関するあらゆるルールを一本化することを目的とした法律を制定した世界初の国の一つとなった。上院の承認を得て当時のジルマ・ルセフ大統領の署名により、2014年4月に施行された[157]。表現の自由やプライバシーといった原則は既にブラジル憲法で保護されているが、新法はこれらの原則がオンライン環境にどのように適用されるかを具体的に規定している。さらに、ネット中立性といった新たな原則を導入し定めている：

---

154 参照先：http://pensando.mj.gov.br/dadospessoais/（最終アクセス日：2016年9月14日）

155 法案、自然人の人格と尊厳を保護するための個人データの処理について。http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/02/Brazil_pdp_ bill_Eng1.pdf （最終アクセス日：2016年9月14日）で閲覧可能。

156 グレン・グリーンウォルド、アンドルー・フィッシュマン、デビッド・ミランダ、「ブラジルにおける新たな政治的地震：メディアはこれを「クーデター」と呼ぶべき時か？」、The Intercept、2016年5月23日、https://theintercept.com/2016/05/23/ new-political-earthquake-in-brazil-is-it-now-time-for-media-outlets-to-call-this-a-coup/。

157 ブラジルインターネット市民権枠組み、http://direitorio.fgv.br/noticia/the-brazilian-civil-rights-framework-for-the-internet で閲覧可能。

第9条：伝送、交換、またはルーティングの責任者は、内容、発信元、宛先、サービス、端末、アプリケーションにかかわらず、あらゆるデータパッケージを平等に処理する義務を負う。

第7条X項において、マルコ・シビルは個人データの保護がプライバシーの観点から重要であり、利用者の要求または当事者間の関係終了後にその削除を要求することを明確にしている。

第7条：インターネットへのアクセスは市民権行使に不可欠であり、ユーザーに以下の権利が保障される：

(X) 特定のインターネットアプリケーションに提供されたあなたの個人データについて、本法に定める義務的なログ保存の場合を除き、ユーザーの請求または当事者間の関係終了時に、最終的な削除を求める権利。

暗号化に関する権利について明文規定はないが、マルコ・シビル法は複数の条項（第7条II項、III項、第11条参照）でユーザー通信の秘密保護を規定している。ただし、これが暗号化を含むかどうかは不明確である。

第7条：インターネットへのアクセスは市民権行使に不可欠であり、ユーザーに以下の権利が保障される：

(II) 法令に基づく裁判所命令による場合を除き、インターネットを通じたユーザーの通信の流れの不可侵性と秘密性；

(III) 裁判所の命令による場合を除き、ユーザーの保存された私的通信の不可侵性と秘密性；

及び

「第11条：接続プロバイダー及びインターネットアプリケーションプロバイダーによる個人データまたは通信データの収集、保存、保持及び処理のいかなる操作においても、これらの行為の少なくとも一つが国内領域で行われる場合、プライバシー権、個人データ保護権、私的通信及びログの秘密保持権を含むブラジル法が義務的に遵守されなければならない。」

ブラジル民間部門における暗号化テクノロジー

他国と比較すると、暗号化は依然としてブラジル企業において軽視されている。このため、立法府は暗号化とプライバシー保護措置の導入を試みている（前述参照）。

一方、多くの企業のセキュリティ態勢は脆弱である。平均的に見て、ブラジル組織がIT予算のうち暗号化テクノロジーに充てる割合は、他国より低い。[158] したがって、ブラジルにおける暗号化の最大の課題は、政府や産業界を含む関連組織による既存手法・基準の導入にあるようだ。

企業が暗号技術を採用する大きな動機は、規制順守に次いで、ブランド保護やデータ侵害による評判被害の回避にある。しかし最近の調査では、回答企業の驚異的な46%が

158 参照：Thales 2016年 グローバル暗号化動向調査：ブラジル編、https://www.thales-esecurity.com/knowledge-base/analyst-reports/global-encryption-trends-study。

ブラジルでは、暗号化計画や戦略が限定的か全く存在しないと認めた企業は驚異的な46%に上った。[159] それらの過半数は、暗号化の使用を決定する責任を持つ機能別リーダーが存在しないと述べた。全体として、IDとアクセス管理、次いでリスクのあるデータの発見が、データ保護における二大優先事項である。[160]

電子政府と参加

市民と政府の現代的な相互作用形態に関して、ブラジルは確立された電子政府モデルを有している。ブラジル公開鍵基盤（Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil）である。[161] これは2001年8月に仮保全措置2.200-2によって導入された。法律自体は主に、関連インフラのセキュリティに焦点を当てている。しかし第10条では、デジタル署名に基づくICP-Brasil証明書の法的有効性を定めている。証明書自体は信頼できる第三者、すなわち認証局によって生成・署名する。証明書には保有者の名前や住民登録番号などのこのデータと、認証局のシグネチャーが記載されている。2010年以降、ICP-Brasil証明書はブラジルIDに部分的に統合可能となり、税務サービス、司法サービス、銀行関連サービスなど様々なサービスに利用できるようになった。実際には、ICP-Brasilデジタル証明書は仮想的な身分証明書として機能し、ウェブなどの電子媒体で行われるメッセージや取引の作成者を安全かつ唯一無二に識別することを可能にする。ただし、統合レベルは依然として低い。

WhatsAppの遮断

最近の出来事として、一部のブラジル裁判所は、メッセージングサービスWhatsAppのブロックを繰り返し命じることで、プライベートメッセージングサービスにおける暗号化に反対する姿勢を示している。[162]完全なエンド・ツー・エンド暗号化に移行して以来、企業に情報提供を要求させるため、裁判所命令によるサービスの一時的な遮断が定期的に行われている。その結果、TelegramやViberなどの他の暗号化メッセージングサービスでは、新規登録者数が急増したと報じられている。Telegramは、遮断が公表されてから数日で100万人以上の新規ユーザーを獲得したと発表した（同サービスの総アクティブユーザー数は1億人を超える）。[163] ブラジル人の中で暗号化通信への需要が広範に存在することは明らかだ。この傾向は、暗号化サービスの利用を阻止しようとする試みによってさらに強まっているようだ。

159 Thales 2016 グローバル暗号化 Trends Study: Brazil, https://www.thales-esecurity.com/knowledge-base/analyst-reports/global-encryption-trends-study.

160 意図したものではなかったかもしれないが、マルコ・シビル法の影響の一部はすでに否定的な形で現れている。インターネットの自由を保護する目的で定められたネット中立性に関する規定は、情報へのアクセスに関してすでに逆効果となっている。民間企業がインターネットへの開放的で無料のアクセスを提供することを禁止しているため、特定のページへの無料アクセスを提供するスマートフォンアプリは同法に反すると見なされている。特に顕著なのは、モバイルデバイスからWikipedia.orgへの無料情報アクセスを促進する『プロジェクト・ウィキペディア・ゼロ』が、マルコ・シビルのネット中立性原則によって禁止されている点だ。

161 詳細はhttp://www.iti.gov.br/icp-brasilを参照のこと。

162 Stephanie Mlot, Brazil Bans WhatsApp (Again) Over Encryption, pcmag, 2016年5月3日, http://www.pcmag. com/news/344200/brazil-bans-whatsapp-again-over-encryption.

163 Telegram Messenger (@telegram)、Twitter、2016年5月2日、https://twitter.com/telegram/status/727200237308227585。

アフリカ地域

本調査ではアフリカ地域における特定の国の暗号化ポリシーについて議論しないことを選択したため、以下に示す証拠はアフリカ大陸の様々な国々に関連するものだ。アフリカ地域は、国家レベルで存在する法的枠組みに関して多様性がある。暗号化ポリシーとその背景に関する証拠を提供するため、本ケーススタディではアフリカ大陸に関する一般的な情報を示した後、アフリカ地域を異なる国々のグループに分類する。これらのアフリカ小地域は、ECOWAS（西アフリカ諸国経済共同体）、EAC（東アフリカ共同体）、COMESA（東部・南部アフリカ共通市場）、ECCAS（中央アフリカ諸国経済共同体）などの地域経済共同体を反映している。

アフリカ連合は、アフリカ大陸（北アフリカを含む）に対して特定の法的・規範的指針を提供してきた地域的な政府間組織である。アフリカ（バンジュール）人権憲章は、1981年にアフリカ連合の枠組みの中で採択するために採択された。[164] バンジュール憲章の監督機能と解釈は、アフリカ人権委員会の任務である。憲章の議定書として、アフリカ人権裁判所を設立する議定書が1998年に採択するために採用され、2005年に発効した。アフリカ連合加盟国の中で、同裁判所への提訴権を認めているのはわずか7カ国である。一方、2016年2月時点で、54加盟国のうち30カ国が議定書を批准している。情報ポリシー分野では、アフリカ連合は「サイバーセキュリティ及び個人データ保護に関するアフリカ連合条約」([165])を採択する。この条約の個人データ保護に関する規定は、概ね欧州のデータプライバシー保護モデルを踏襲し、個人データ処理のセキュリティに関する複数の規定を含む。市民社会によるイニシアチブでは、「大陸全体のインターネットポリシー立案とガバナンスへのアプローチ形成を支援する」ことを目的とした、アフリカ独自の「インターネット上の権利と自由に関する宣言」が採択するために採用された。([166])

英連邦やフランコフォニーなどの国際政府間組織、及び国際電気通信標準化機関が推進するモデル法の影響は、本報告書で議論される具体的なポリシーに重大な影響を与え得るが、その影響分析は本研究の範囲を超える。

アフリカのインターネットユーザー率は依然として世界平均を大きく下回っており、これが関連法規の（相対的な）不足を説明している。世界の他の地域では2015年時点で、全人の約50%がインターネットユーザーであるのに対し、アフリカ大陸は28.6%にとどまっている。([167]) 進行中のモバイル革命によってこの数字は変化すると予想されるが、インターネットポリシー分野における最大の課題は、インターネットへのアクセス確保であり続ける可能性が高い。

---

164 アフリカ（バンジュール）人権・人々 の権利憲章、1981年6月27日採択するために採用する、OAU文書CAB/LEG/67/3 rev. 5、21 I.L.M. 58 (1982)、1986年10月21日発効。

165 アフリカ連合サイバーセキュリティ及び個人データ保護条約、2014年6月27日に採択するために採用された。現在、加盟国8カ国が署名している。

166 アフリカインターネット権利・自由宣言を参照のこと。http://africaninternetrights.org/（最終アクセス日：2016年9月14日）。

167 インターネット世界統計、http://www.internetworldstats.com/stats1.htm（最終アクセス日：2016年9月14日）。

北アフリカ[168]

北アフリカ地域の各国では、2011年に始まった変革期において、暗号化を隠匿する法的措置が顕著に増加したわけではない。しかし、立法は変革以前にさかのぼることが多いものの、その執行はその後厳格化している。チュニジアのように革命が成功し政権交代を経験した国々と、そうでない国々との間で、暗号技術に対する姿勢に差異は見られない。

チュニジアにはオンライン上の匿名性を制限する複数の法律が存在する。2001年電気通信法の第9条及び第87条は暗号化技術の使用を禁止し、無許可での販売・使用に対しては最高5年の懲役刑を規定している。[169] これらの法律は旧政府下で制定されたものの、関連規定を緩和する動きはこれまで成功していない。しかしながら、これらの法律が執行されたという最近の報告もない。それでも、これらの法律の存在が確認されていることは、メディアや通信環境における暗号技術の使用に対して、より寛容なアプローチを取ることに国が躊躇している証拠とみなすことができる。

アルジェリアでは、2012年以降、暗号テクノロジーの利用には関連通信当局であるARPT（郵便・電気通信規制庁）からの法的認可が必要となっている。[170] エジプトでは、2003年電気通信規制法第64条において、NTRA（国家電気通信規制庁）、軍、国家安全保障当局の書面による同意なしに暗号化デバイスを使用することは禁止されている。[171] この法律は以前の時代に制定されたものの、現在も有効である。さらに、インターネットカフェのユーザーはインターネットにアクセスするためにPINを取得する必要がある。そのため、名前、メールアドレス、携帯電話番号を登録しなければならない。国家安全保障が問題となる場合、これらのオンライン情報はすべて、裁判所の事前同意なしに大統領府、治安機関、情報機関、行政管理する当局によってアクセス可能である。

エジプトは「リモートコントロールシステム」と呼ばれるソフトウェアを使用していると報じられている。このソフトウェアは、対象のコンピューター上のデータを取得し、暗号化されたインターネット通信を監視し、スカイプ通話、電子メール、メッセージ、ブラウザに入力されたパスワードを記録し、遠隔でデバイスのウェブカメラとマイクを起動することができる。[172] 2015年末にエジプトがFacebookの「フリーベーシックス」サービスを遮断した際、Facebookユーザーのデータアクセスに関する協力が得られなかったことが報じられている。[173]

---

168 SMEXの「デジタルの権利に影響を与えるアラブ諸国の立法と命令」プロジェクトは、暗号化問題に特化していないものの、当該地域の関連法に関する参考情報を提供している。詳細はhttps://smex.silk.co/（最終アクセス日：2016年9月14日）を参照のこと。

169 2001年1月15日付第1-2001号法（通信法公布に関する法律）（チュニジア）、http://www.wipo.int/wipolex/en/text.jsp?file_id=204160（最終アクセス日：2016年9月14日）。

170 2012年6月11日付決定第17号、http://www.arpt.dz/fr/doc/reg/dec/2012/DEC_N17_11_06_2012.pdf（最終アクセス日：2016年9月14日）。アクセス日：2016年9月14日）。

171 エジプト電気通信規制法（翻訳）、http://hrlibrary.umn.edu/research/ Egypt/Egypt%20Telecommunication%20Regulation%20Law.pdf（最終アクセス日：2016年9月14日）。

172 Citizen Lab,「ハッキング・チームの『追跡不能』スパイウェアの分布図」, モンク国際問題大学院, 2014年2月17日、https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/（最終アクセス日：2016年9月14日）。エミール・ナデル「新たなリークで明らかになったエジプトのハッキングソフトウェア購入」デイリーニュースエジプト、2015年7月6日、http://www.dailynewsegypt.com/2015/07/06/egypts-purchase-of-hacking-software-documented-in-new-leaks/（最終アクセス日：2016年9月14日）。

173 ヤスミン・アブタレブ、ジョセフ・メン「独占：エジプト、監視を理由にFacebookのインターネットサービスを遮断ー情報筋」ロイター、2016年4月1日、http://www.reuters.com/article/us-facebook-egypt-idUSKCN0WY3JZ（最終アクセス日：2016年9月14日）。

モロッコでは、暗号テクノロジー（ソフトウェア・ハードウェアを問わず）の輸出入には政府の許可が必要だ。関連法である第53-05号法（法的電子データ交換に関する法律）は2007年12月に施行された。第13条は次のように定めている：

> *違法目的での使用を防止し、国防及び国家の内外における安全保障上の利益を保護するため、暗号化サービス手段の輸入、輸出、供給、運用又は使用は、以下の条件に従うものとする：a) 当該サービスの利用が、電子的に伝送されるデータの真正性確認又は完全性確保を唯一の目的とする場合、事前届出を要する。b) 上記a)に定める目的以外の目的の場合、政権による事前承認を要する。*

第32条、第33条及び第34条は、第13条違反に対する罰則を規定しており、1年の懲役及び100,000 MAD（約10,000米ドル）の罰金に相当する。2015年2月以降、暗号化テクノロジーの承認・監視を担当する関連当局は民間機関ではなく、軍事機関であるDGSSI（情報システム保安総局）となった。[174]

結論として、北アフリカ諸国では政府の監視を優先して暗号化を制限する傾向が認められる。暗号化テクノロジーの使用は禁止されるか、厳しく制限されている。

東アフリカ

東アフリカ地域では、暗号化テクノロジーを使用することを制限する具体的な規定は施行されていないようだ。しかしながら、国家の監視権限は拡大傾向にある。他のアフリカ諸国と同様、主な理由はテロ攻撃の防止である。ソマリアに近いケニアは、この脅威を理由に、制限措置を採択するためにしている。同国は最近、2016年末に採択するために『コンピュータ及びサイバー犯罪法』を迅速に審議している。[175] 欧州サイバー犯罪条約に基づくこの法案は、捜査における法執行機関のデータアクセスに関連し、暗号化に関する具体的な規定を含む。これらの規定は、復号能力を有するサービスプロバイダーに対し、保存された情報及び通信の復号命令を発する権限を認めている。オンライン活動に関する厳格な法律で知られるエチオピアでは、テロ容疑で起訴された複数のブロガーが通信の暗号化も非難された。[176]

ウガンダでは過去3年間に複数の法律やICTポリシーが制定されたが、いずれも暗号化には触れていない。2016年の大統領選挙後、ウガンダ政府はTwitterやFacebookなどのソーシャルネットワークを遮断した。

---

174 Bulletin officiel n° 6332 du 15 rabii II 1436 (2015年2月5日)、http://adala.justice.gov.ma/production/html/Fr/liens/..%5C188896.htm (最終アクセス日: 2016年9月14日)。

175 参照：MyGov、「コンピューター及びサイバー犯罪法が年末までに施行予定」、2016年6月29日、http://www.mygov.go.ke/?p=10848（最終アクセス日：2016年9月14日）。

176 Endalk Chala「エチオピア対Zone9ブロガー裁判：判決は7月20日予定」Global Voices Advox、2015年7月17日、https://advox.globalvoices.org/2015/07/17/what-you-need-to-know-about-ethiopia-v-zone9-bloggers-verdict-expected-july-20/ (最終アクセス日: 2016年9月14日)。参照：フリーダムハウス『ネット上の自由 2015：エチオピア』https://freedomhouse.org/sites/default/files/resources/FOTN%202015_Ethiopia.pdf（最終アクセス日：2016年9月14日）。

また、WhatsAppも同様である。[177] エンド・ツー・エンド暗号化を使用するサービスとその他のサービスとの間に違いはなかったようだ。多くのユーザーが制限を回避するためにVPNサービスの利用を選択したため、これらの制限措置の影響を受ける範囲を制限することができた。

西アフリカ

アフリカ大陸で最も人口の多いナイジェリアは、現在アフリカ全体で最多のインターネットユーザー数を誇る。51%の人がインターネットを利用している。[178] ガーナやコートジボワールなどの国々では、人々における「オンライン」人の割合はわずか20%程度と報じられている。[179]西アフリカ諸国は暗号化テクノロジーやその輸出入、および使用を制限していないように見えるが、ほとんどの国内外企業は依然として通信にVPNを利用している。

ガーナは最近、犯罪防止を名目に市民の電子通信及び郵便通信を傍受する法案を提出した。法案セクション4(3)項は、公務員の口頭命令のみで政府があらゆる通信を傍受することを許可している。[180] 他のセクションでは司法判断を必要とする規定があるものの、セクション4(3)項はこれら全てを無効化し、実質的に裁判所命令なしの通信監視を政府に無制限に認めている。こうした懸念を踏まえ、国連人権委員会はガーナに対し、法案の濫用を防ぐ法的保護措置を講じるようする([181])

最近、ナイジェリア通信委員会は通信合法傍受規制に関する法案を起草した。[182]この法案が可決されれば、司法監督や裁判所命令なしに全ての通信を傍受することが可能となり、携帯電話企業は音声・データ通信を3年間保存することを義務付けられる。さらに、草案は国家安全保障機関に全ての暗号化通信を復号するための鍵を要求する権利を与える計画だ。具体的には、法案草案セクション13(1)項は次のように規定している：

> *傍受対象の通信が暗号化または保護された通信である場合、免許取得者は国家安全保障顧問および国家保安局に対し、当該保護または暗号化通信への鍵、コード、またはアクセス権を提供しなければならない。*

西アフリカ地域の他国ではインターネット利用率が著しく低く、トーゴの5%強からコートジボワールの20%超まで幅がある。[183]

---

177 参照：BBCニュース「ウガンダ選挙：Facebookとワッツアップが遮断」2016年2月18日付、http://www.bbc.com/news/world-africa-35601220（最終アクセス日：2016年9月14日）。参照：Nshira Turkson, 「ウガンダ大統領選挙におけるソーシャルメディア遮断」, The Atlantic, 2016年2月18日, http://www.theatlantic.com/international/archive/2016/02/uganda-election-social-media-shutdown/463407/ (最終アクセス日: 2016年9月14日最終アクセス）。

178 参照：インターネット・ワールド・スタッツ、http://www.internetworldstats.com/stats1.htm（最終アクセス日：2016年9月14日）。

179 参照：インターネット・ワールド・スタットス、http://www.internetworldstats.com/stats1.htm（最終アクセス日：2016年9月14日）。

180 アジボラ・アディグン、「スパイ法案導入によるガーナの自由への侮辱」、Student For Liberty、2016年3月29日、https://studentsforliberty.org/africa/2016/03/29/affront-on-freedom-in-ghana-with-the-introduction-of-spy-bill/ (最終アクセス日: 2016年9月14日)。

181 News Ghana、国連、ガーナのスパイ法案に関する統計を要求、2016年3月11日、https://www.newsghana.com.gh/ un-demands-statistics-on-ghanas-spy-bill/ （最終アクセス日：2016年9月14日）。

182 ナ イ ジェリア通信委員会、通信合法傍受規制草案、http://bit.ly/1du7UKO（最終アクセス日：2016年9月14日）。

183 参照：インターネット・ワールド・スタッツ、http://www.internetworldstats.com/stats1.htm（最終アクセス日：2016年9月14日）。

南部アフリカ[184]

南アフリカのユーザーは暗号化の使用を禁止されていない。[185] ただし、当該テクノロジーの提供は2002年電子通信取引法によって厳格に規制されている。[186] 暗号化テクノロジー提供者は通信省長官への登録が必要であり、監督または管理責任を有する信頼できる担当者の詳細な経歴書の提出を含む。違反に対する罰則は最長2年の禁固刑に至る。

2003年以降、「通信傍受及び通信関連情報提供規制法」が施行されている。[187] これにより警察は、裁判所命令に基づき暗号化された通信の復号を要求する力をもつ。裁判所命令の受領者は、復号化キーの提供、あるいは少なくとも復号化への協力を通じてこれに従わなければならない。罰則は、200万ランド（約14万米ドル）から最高10年の懲役、企業の場合は500万ランド（約34万米ドル）の罰金の上限が定められている。

中央アフリカ

コンゴ民主共和国、中央アフリカ共和国、ガボン、カメルーンなど中央アフリカ諸国では、インターネットポリシー問題に対処する法制度がまだ十分に整備されていない。インターネットは比較的規制の緩い領域のままである。オンラインメディアの利用を制限したり、暗号化テクノロジーの使用を禁止したりする実際の法律は知られていない。コンゴ民主共和国では人口の3%、中央アフリカ共和国では4%、カメルーンでは11%がインターネットのアクティブユーザーである。([188])

5. 暗号技術に関連する人権枠組み

表現の自由とプライバシーに関する国際人権文書

デジタルテクノロジーは広範な人権に影響を与えるが、表現の自由（市民的及び政治的権利に関する国際規約［ICCPR］第19条）と私生活の権利（ICCPR第17条）は、暗号手法の保護に特に関連性が高い。国際的な「ソフトロー」である世界人権宣言（UDHR）とは異なり、ICCPRは法的拘束力を持つ国際条約である。([189])

---

184 南部アフリカ地域の他の4カ国（ボツワナ、ナミビア、レソト、スワジランド）については特に関連する情報が見つからなかったため、提示された証拠は南アフリカのみに関するものである。

185 参照：フリーダムハウス『Freedom on the Net 2015: South Africa』https://freedomhouse.org/report/freedom-net/2015/south-africa（最終アクセス日：2016年9月14日）。

186 参照：電子通信取引法、2002年法律第25号、http://www.internet.org.za/ect_act.html（最終アクセス日：2016年9月14日）。

187 通信傍受及び通信関連情報提供の規制に関する法律、政府官報、第24286号、2003年1月22日、2002年法律第70号、http://www.internet.org.za/ricpci.html（最終アクセス日：2016年9月14日）。html（最終アクセス日：2016年9月14日）。

188 参照：インターネット世界統計、http://www.internetworldstats.com/stats1.htm（最終アクセス日：2016年9月14日）。

189 トビー・メンデル。*国連意見及び表現の自由特別報告者：表現の自由に関する国際基準の漸進的発展*。マクゴナグル及びドンダース編『国連と表現及び情報の自由』第8章、238頁。

以下の分析は普遍的な人権システムに焦点を当てるが、有用な場合には地域的・国家的権利のために展開された議論も活用する。

表現の自由[190]、情報への自由を含む、は人々が思想や情報を送受信する権利を保護する[191]。意見を持つことは受動的行為であり絶対的自由である一方[192]、表現の自由の権利には情報と思想を求め、受け取り、伝える活動が含まれる[193]。情報へのアクセスは自由な意見形成の前提条件である。意見の自由（第19条(1)）とともに、第19条(2)は自己啓発にとって「不可欠」であり、「あらゆる社会にとって本質的」であり、「あらゆる自由で民主的な社会の礎石」と見なされている。[194] フランク・ラ・ルーは、表現の自由をICCPRの下で享受される他の多くの権利の「実現手段」として正しく言及している。[195] 表現の自由と情報の権利において、保護される事項は相互依存性によって特徴づけられる。情報は表現の基盤であるが、表現もまた情報を生み出し、普及させるのである。[196] 表現の自由に対する制限は、第19条第3項の条件下でのみ許容される。制限は法律で定められ、かつ以下のいずれかに必要であること：(a) 他者の権利または名誉の尊重のため、または (b) 国家安全保障、公共の秩序、公衆衛生または公衆道徳の保護のため。さらに制限の可能性はICCPR第20条に規定されている。[197] 暗号技術への制限においては、その根拠はほとんどの場合、第19条3項(b)、すなわち国家安全保障と公共の秩序へのリスクに基づく。これは個人の安全保障（例えば個人の電子通信への干渉からの保護）と国家安全保障との関係、及びその区別という複雑な問題を提起する。両者は必ずしも同一ではなく、むしろ異なる場合が多い。政府が国家安全保障を強調するあまり、コンピューターセキュリティや人間の安全保障の技術的定義を軽視する危険性がある。[198]

ICCPR第19条は、あらゆる形態の視聴覚的表現、ならびに電子的・インターネットベースの表現手段に適用される。[199] したがって、この規範の文言は社会技術的発展に対応する余地を明らかに有している。第19条はまた、インターネット上の通信慣行や様々な仲介サービスを保護する。情報伝達サービスだけでなく、通信を可能にするサービスも含まれる。[200] インターネットは、比較的低い参入障壁と、表現の自由と情報の自由の形態を決定するインターネットベースの主体への提供可能性により、多方向的なコミュニケーション活動に前例のない可能性を秘めている。[201] 主な役割の重要性

190 ICCPR第19条；ACHR（アラブ人権憲章）第32条；ACHR（米州人権条約）第13条；ACHPR（アフリカ人権と人々 の権利に関する憲章）第9条；AHRD（ASEAN人権宣言）第23条。

191 サラ・ジョセフ、メリッサ・カスタニ著『*市民的及び政治的権利に関する国際規約*』第3版、オックスフォード、2013年、590頁。

192 ドミニク・マクゴールドリック著『*人権委員会*』クラレンドン・プレス、1994年、460頁。

193 一般意見34/11。

194 CCPR/G/GC/34、§ 2（参照事例：マルケス・デ・モライス対アンゴラ、1128/2002；ベンハジ対アルジェリア、No. 1173/2003；パク・テフン対大韓民国、No. 628/1995）。

195 A/HRC/17/27、§ 23。参照：Michael O'Flaherty、前掲書、58頁以降。

196 ターラック・マクゴナグル著『マクゴナグル＆ドンダース編：*国連と表現の自由及び情報の自由*』第1章、3頁。

197 マンフレッド・ノヴァク『市民的及び政治的権利に関する国際規約解説』第2版、477頁。参照：マイケル・オフラハティ『市民的及び政治的権利に関する国際規約：現在と未来のための表現の自由及び情報の自由基準の解釈』マクゴナグル・ドンダース編『*国連と表現及び情報の自由*』第2章、69頁以下。

198 議論についてはニッセンバウム2005を参照せよ。

199 CCPR/C/GC/34、§ 12。

200 ヨゼフとカスタンの前掲書、599頁。

201 ターラック・マクゴナグル。同上。5頁。

したがって、公の議論における司会者や主要なゲートキーパーの役割は、もはや伝統的なメディアに主に割り当てられていない。とはいえ、伝統的なメディアは依然としてジャーナリズムコンテンツの主要な供給源であり、より広範なアジェンダを設定している。[202]

表現の自由にとって構造的に重要であるため、ジャーナリズムコンテンツを不当な干渉から保護する全プロセスは第19条の適用対象となる。さらにこれは、制限が合法となるのは、当該国家が重要な公共的・私的利益に対する具体的かつ差し迫ったリスクを立証できる場合に限られることも意味する。この評価に基づき、仲介業者も、自ら「発言」を行わなくても、他者のコミュニケーションにとって構造的に重要であるため、表現の自由の保護を享受し得る。これについては後述するが、特に暗号化へのアクセスにおける仲介業者の役割に関して詳しく説明する。

プライバシー権[203]は、個人のプライバシー、家族、住居、通信に対する「恣意的または違法な干渉」から保護する。加えて、ICCPR第17条(1)は、個人の名誉と評判に対する「違法な攻撃」から保護する。第17条の適用範囲は広い。プライバシーは、自己に関する情報を管理する権利として理解できる(204)。法律が定める範囲内で、自らの望む通りに生活する可能性は、他者が私たちについて持ち、私たちに対する行動の指針として使用する情報に実質的に依存する。これが、プライバシーを人権として保護する中核的な正当性の根拠の一部である。

プライバシーの権利に関する規定は、保護範囲の新たな現れを許容する。[205] 実際、この規定が起草された当時、ネットワーク通信の台頭は想定されていなかった。しかし、第17条(1)の「通信」というコンセプトは、論理的に、電子メールやTwitterなどのプラットフォーム上のダイレクトメッセージといった新たな形態の私的電子通信の完全性と秘密性を包含する。(206) 電子通信が情報及び思想の探求、アクセス、伝達の自由を促進する限りにおいて、プライバシーと表現の自由の間には密接な相互関係がある。同様に、情報の機密性や完全性を確保するために暗号化手法が用いられ、それによってプライバシー権利の保護が強化される場合、その保護はこうした新たな安全な通信形態にも拡張され得るのである。(207) そうして初めて、不当かつ不合理な侵入からの真の自由が語れるのである。(208)

ICCPR第17条の保護は、思想・結社・信教の自由（これらは別個の権利としても保護されている）の実現にも寄与する。このように、プライバシーは他の権利の享受を可能にするという広く認められた特質を有しており、この点は表現の自由の権利と共通する。学術的観点からは、ヴォリオが「すべての人権はプライバシー権の一側面である」と主張している。(209) この考えはリーガンによって再確認されている。(210)

---

202 参照：ターラック・マクゴナグル、前掲書。

203 ICCPR第17条；ACHRA（アラブ）第21条；ACHRA（アメリカ）第11条；AHRD第21条。

204 チャールズ・フリード『プライバシー』（1968年）77 *イェール・ロー・ジャーナル*475頁、483頁参照。

205 F. ヴォリオ『人格、プライバシー、家族』197頁、L. ヘンキン編 *『国際人権章典』*ニューヨーク：コロンビア大学出版局1981年所収。これは欧州人権条約第8条にも同様に当てはまる。例えば欧州人権裁判所2008年12月4日判決（申請番号30562/04）§66を参照。同判決は欧州人権裁判所の判例を含む保護領域の概要を示している。

206 一般意見16/32、§8。マンフレッド・ノヴァク、前掲書、401頁。

207 Wagner 2012も参照せよ。

208 SE ウィルボーンの定義を参照。Georgia Law Review 32 (1998), pp. 825, 833。

209 F. ヴォリオ、前掲書、193頁。

210 リーガン1995を参照せよ。

これらの権利を侵害しない義務に加え、国家は、その管轄下にあるすべての個人の表現の自由及びプライバシーの享受を効果的に保障する積極的義務を負う。[211] プライバシー権に関するICCPR第17セクション第2項は、立法その他の措置を通じて市民を干渉から保護するよう国家に明示的に命じている。[212]この権利は、国家機関からであれ自然人・法人からであれ、あらゆる干渉や侵害に対して保障されねばならない。[213] 重要なのは、通信の秘密性と完全性が法的に（de jure）かつ事実上（de facto）保護されるべきであり、[214] 公的当局と民間団体双方のデータ処理が条約に準拠するよう、効果的な措置が講じられる必要がある点だ。[215]

これら関連する人権の下で特定の暗号化方式の保護を検討する際には、暗号化の技術的アプリケーションと、通信・情報・計算における人間向けの特性とを区別することが重要である。前述の通り、これらの特性には秘密性、プライバシー、真正性、可用性、完全性、匿名性が含まれる。通信及び情報保存・処理ツールのこうした特性こそが干渉からの保護に値する。なぜならこれらの特性こそが、国際人権法で保護される権利の実現を可能にするからである。したがって欧州評議会議閣僚委員会は、暗号化の禁止や弱体化をインターネットの自由に対する逆行的措置と位置付けている。[216]

表現・意見の自由と私生活の権利（私的通信の権利を含む）は、特定の状況下で衝突しうる。当初から、第17条セクション2に基づく積極的義務が検閲の認可につながるべきでないこと、また私生活の権利と表現の自由の権利が相互依存関係にあることが認識されていた。[217] 表現の自由は、表現が自然人に関連したり影響を与えたりする場合には、私生活の権利の保護を妨げる可能性があるが、これを尊重しなければならない。さらに別の関連性がある。コミュニケーションの文脈における基本的な人間の必要性は、情報を伝達・受領し、自己の人格を発達させることである。この点で意味を持つためには、コミュニケーションの過程は、問題となっている両方の権利に及ぶ一定の規範的要件を満たさなければならない。

前述の表現の自由の例で述べたように、これらの権利は、個人の尊厳、平等、生命や安全といった他の権利や利益、あるいは正当な公共の利益と衝突する可能性がある。こうした場合、各権利や価値の完全性は最大限に維持されなければならず、均衡を図るために必要な要件は、合法的な目的（他者の権利、公衆道徳、国家安全保障など）を考慮して、法律に基づく必要かつ比例的な（特に制限が最小限の）ものでなければならない。

---

211 CCPR/G/GC/34、§11。

212 一般意見16/1。

213 一般コメント16/1。

214 ノヴァクはさらに、ICCPR第17条に基づく通信及び電気通信の秘密の保護は、民間企業が情報伝達システムを運営するケースにも及ぶと指摘している。参照：M. ノヴァク、p. 401。

215 一般意見16/32、§8 - §10。

216 インターネットの自由に関する閣僚委員会の加盟国への勧告 CM/Rec(2016)5。2016年4月13日。https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa、ポイント4.1.7. および 4.2.5.

217 M.J. Bossuyt, 『市民的及び政治的権利に関する国際規約の「準備作業」ガイド』, ドルドレヒト: Nijhof 1987, p. 346, 人権委員会第9回会合, E/CN.4/SR.374, p. 12-15 を参照.

「妨げられない通信」の保証

フランク・ラ・ルーによる表現の自由の構造的重要性の評価を踏まえ、通信プロセスを実質的に「自由」たらしめる法的・事実上の前提条件の本質的特徴を特定することが重要である。暗号化技術の利用可能性によって強く促進される本質的要件の一つは、「妨げられない通信」の要件と呼べるものである。暗号化は、人々が通信の完全性、可用性、機密性を保護することを可能にすることで、この通信様式を支える。妨げられない通信の要件は、通信の自由にとって重要な前提条件であり、米国最高裁判所(218)、ドイツ連邦憲法裁判所(219)、欧州人権裁判所(220)などの憲法裁判所によって確認されている。

より具体的には、意味のあるコミュニケーションには、人々のが自身のニーズに応じて情報を選択し、考えを発展させ、言語様式を決定し、コミュニケーション手段を選定する自由が不可欠である(221)。検閲手段の強制とその表現の自由への影響は、この権利の重要な側面と特性に対する悪影響の一例である。伝達経路の安全性を妨害して偽造された内容を提供することは、表現者が伝えたかった内容を歪める。第三者が通信を監視しているという認識は、コミュニケーションの様式を変える可能性がある。(222) 市民は表現方法を変える選択をし、検閲官を欺こうとしたり、自己検閲によって特定の問題について完全にコミュニケーションを控えることさえある。後者は、抑制されないコミュニケーションの条件がもはや存在しない場合、「萎縮効果」がコミュニケーションの歪みとして現れる可能性を示している。

抑制されないコミュニケーションは自律的な人格形成の前提条件でもある。人間は他者との交流を通じて人格を成長させる。[223] 国連初のプライバシー特別報告者であるジョー・カナタチ教授によれば、プライバシーは単なる手段的権利ではなく、人格の自由かつ妨げられない発展という包括的な基本的権利の達成を可能にする本質的権利である。[224] このようなコミュニケーションが阻害される場合、発言は発言者の真の（最も内なる）個人的見解を反映するだけでなく、そもそもコミュニケーションを形成するものではない考慮事項によって不当に影響される可能性があるため、相互作用は偏る。したがって、社会的相互作用を通じて人格を形成するプロセスは妨げられる。

こうした混乱による制限的な影響は、個人の情報や考えの自由な表現に直接的な影響を及ぼす。さらに、抑制のないコミュニケーションの条件がもはや存在しなくなった場合、それは社会全体のコミュニケーションや表現の風土に影響を与える可能性がある。したがって、「抑制のないコミュニケーション」の欠如は、知的活動の全般的な麻痺や凍結をもたらす可能性がある。[225] このようなより一般的な影響により、妨げとなる国家の行為は

---

218 例えば、ニューヨーク・タイムズ社対サリバン事件（376 U.S. 254 (1964)）およびドンブロウスキー対フィスター事件（380 U.S. 479 (1965)）を参照のこと。

219 BVerfG NJW 1995、3303 (3304) および BVerfG NJW 2006、207 (209) を参照のこと。

220 Cumhuryiet Vafki 他対トルコ、ECHR 10.08.2013 - 28255/07; Ricci 対イタリア、ECHR 10.08.2013 - 30210/06。

221 参照：一般意見16/8。

222 一般コメント34が強調するように、プライバシーと表現の自由の間には相互関係がある。アメリカ人の視点からは、Canes-Wrone/Dorf, NYU Law Review 90 (2015), 1095 et seq.を参照せよ。

223 Tarlach McGonagle.『国連と表現の自由及び情報の自由』第1章、3頁。

224 プライバシー権利に関する特別報告者ジョセフ・A・カナタチの報告書、A/HRC/31/64。

225 シルヴィ・クードレー『国連と表現の自由及び情報の自由』第7章、258頁を参照。

「抑制されない通信」の可能性自体が、表現の自由に対する重大な制限である。さらに、暗号化テクノロジーの使用は表現の自由の権利（「暗号化の権利」）の範囲内にあるという見解を支持する。ドイツ連邦憲法裁判所による「IT基本権」[226]に関する判決例は、テクノロジー変化を踏まえた基本権利の拡張可能性を同様の観点から支持し、実証している。同裁判所は比喩的に言えば、個人の人格の一部がITシステムに移行するため、適用される保護もそれに伴って移行すべきだと認めている。

暗号化の使用・展開を制限する国家措置は「抑制されない通信」を制限する傾向があるため、効果的な人権保護のこのコンセプトには、テクノロジーによって自己を保護する市民の可能性を含めるべきだという強い主張が可能だ。複雑な社会において、表現の自由は単に発言する権利があるだけでは実現しない。自己表現の権利を行使する前提条件を保護する第二段階の保証が必要である。監視のリスクがある場合、暗号化によって言論の自由を保護する権利は、この第二段階の権利の一つとみなされるべきだ。したがって、暗号化そのものの利用可能性や有効性を制限することは、私生活や通信を保護する表現の自由とプライバシー権への干渉を構成する。ゆえに、合法性、必要性、目的に基づいて評価されなければならない。

手続き的側面：透明性の保証

表現の自由とプライバシー権（私的通信の権利を含む）は実質的性格を有し、特定の行為や個人の状態を実質的に保護する。基本権理論において、実質的権利は効果を発揮するために手続き的保証によって補完されなければならないことは確立されている。[227] こうした手続き的保証には、実効的な救済を受ける権利などの権利が含まれる。しかし、これらの手続き的権利は、実質的権利と同様に、政府による特定の手続き的義務を伴わなければならず、それがなければ権利は侵食されることを確認することが重要である。

ICCPR（市民的及び政治的権利に関する国際規約）及びUDHR（世界人権宣言）における市民的・政治的権利は、古典的には少なくとも主に、国家による干渉からの自由として認識されてきた。[228] これらは否定的権利として概念化されている。つまり、国家が特定の行動を控えることを要件とする権利である。先に論じたように、これらの権利はある程度、積極的な行動も要件とする。これには非政府組織による権利侵害からの保護も含まれる。[229] もちろん、ICCPR条約が直接拘束するのは国家のみであるため、基本的人権を行使するには国家の作為または不作為が必要だ。同時に、国連ビジネスと人権に関する指導原則は、民間主体に対し事業活動における人権尊重を求めている。

この観点から国家の行動を見ると、多くのポリシー分野で法的ガバナンスの様式が変化していることに注目すべきだ。こうした法的ガバナンスは、国家と市民の垂直的関係における伝統的な線形的規制形態とは特徴づけられないことが多い。むしろ国家と非国家アクターのネットワークの中で行使され、法的規範のみならず非公式な手段にも基づいているのだ。[230]

---

226 BVerfG NJW 2008, 822.
227 参照：ロバート・アレクシー、ジュリアン・リバース『憲法上の権利の理論』315頁以降。
228 ヘルデゲン『国際法』§47 序文1項。
229 参照：シーダーマイアー『国際的基礎権としての私的領域の保護』74頁。
230 例えば参照：ロイゼランド『非公式政府』『政治学百科事典』1018頁。

これは、現在のグローバル化した環境における情報テクノロジーおよびサービスに関して特に当てはまる。

こうしたネットワーク化されたガバナンス体制（非公式な手段を含む）は、規制目標の達成に極めて効果的である。しかし人権の観点からは、リスクも引き起こす。ガバナンスシステムがますます複雑化し、国家主体が人権に敏感な分野で民間主体と非公式に連携する場合[231]、責任の拡散や不明瞭化が生じるリスクがある。市民は特定の結果や認識された不正義について、誰に責任を追及すべきか分からない。したがって、実質的権利は、少なくとも市民が以下の点を評価できる程度に、政府システムの透明性を確保する義務も含むように解釈されなければならない。(1) 誰が決定を下したか
(2) どのような措置が取られたか。

これは、暗号化に関して様々な管轄区域で政府が仲介業者やその他の業界関係者との間で行う協議に極めて関連する。これらの協議とその結果は、国家が正式な措置を取らず、単に業界との協力に依存して、合法性、必要性、正当な目的の評価にかかわらず、要求されるたびにあなたのデータや暗号化キーを引き渡すシステムにつながる可能性がある。この場合、法的審査の対象となる法令が存在しないため、人権保護の手続き的側面においては透明性が求められる（その他の手続き的・実質的保障は別として）。国家は、こうしたネットワーク化された取り決めと、それらが安全な暗号手法・テクノロジーがもたらす自由な使用・導入に課す制限について、透明性を確保する義務がある。いわゆる「口止め命令」が発令されると、逆の結果が生じる。こうした命令は、業界がデータ主体だけでなく一般市民に対しても、意図的な権利侵害について知らせることを妨げる場合が多い。この点において、透明性の要請は、単に闇から物事を明らかにし説明責任を確保するための一般的な要請以上のものだ。それは、基本的人権に対する危険性を認識し、それぞれの自由を行使するための前提条件である。

国家、ユーザー、サービスプロバイダー：安全保障の仲介業者

ユーザーはデータの安全性をサービスプロバイダーに依存しているため、デジタル領域における人権保護の観点からも、これらのサービスプロバイダーを規制する法的枠組みを特に慎重に検討することが重要だ。本研究の第2セクションでは、エンドユーザーの利益のために暗号技術が導入される多様な形態を既に示した。この概観から明らかなように、ユーザー自身が保護策を講じる可能性を除けば、人権保護の実現にはサービスプロバイダーの主導と関与が要件である。クラウドベースサービスのユーザー監視に関して言えば、多くの点で「ユーザーは自らを保護できず、基本権利の享受と国家安全保障による恣意的な干渉からの保護をサービスプロバイダーに依存している」のである。[232] こうしたサービスプロバイダーは、しばしば様々な形態のユーザーの表現やコミュニケーションを促進する仲介業者として機能する。[233] ユーザーは、自身の情報と通信の完全性、可用性、機密性を確保する適切な最新技術的措置をサービスプロバイダーが講じることを信頼できるべきである。したがって国家は、メディア・通信プラットフォームやサービスが安全な暗号化手法を利用できる能力を妨げてはならない。むしろ、

231 参照：Tarlach McGonagle. 前掲書 第1章 p. 39.
232 Arnbak 2016年を参照。
233 マッキノン他、ユネスコ研究；参照：カロル・ヤクボヴィッチ『初期段階：国連、ICT、表現の自由』『*国連と表現・情報の自由*』第10章、324頁以降。

法的枠組みは、サービスプロバイダーに対する義務を規定するか、少なくとも彼らにそうするよう促すべきである。例えば、データ保護・セキュリティ法において技術的な最低基準を設定したり、ユーザーに実装された保護レベルを示すデータセキュリティ認証を確立したりする方法がある。いずれにせよ、仲介業者がユーザーのプライバシー保護のために講じる措置は、それらの自由を実質的に保護する上での構造的重要性から、ICCPR第19条及び第17条の両方の適用範囲に含まれる。

暗号ポリシーに関する議論において、政府による合法的なアクセス権限、および人権を尊重するためにそのようなアクセスが行われるべき条件というこの疑問は、垂直的かつ国家的な焦点を持つ。ここで意味するのは、この議論が自国の社会成員に対する国家の義務と責任、ならびにそれに応じて定めるものとする法律や規制について、人権を尊重しながら扱っているということである。したがって各国において、アクセスに関する懸念は主に「正当な権限を持つ当局のアクセス不足」に集中する傾向がある。しかし十分に確認されていない事実として、議論の対象となるサービスやツールは国境を越えて存在する。[234] 同様に、政府やその他の主体が国境を越えて情報や通信へのアクセスを得ようとする場合も同様である。国際的側面と越境アクセスの可能性は、実際にはデータ保護やサイバーセキュリティポリシーの脅威モデルに外国のアクターを含めるべきことを意味する。[235] これが、政府によるデータへの越境アクセスを制限・形成するために暗号化手法が積極的に模索される理由の一つだ。

合法的な政府アクセスにおける管轄権の複雑さは重大であり、未だ解決されていない難題である。特に、従来の合法的な政府アクセスは、強力な地域的結びつきを持つ通信事業者を標的とするデジタル通信へのアクセスから、サービスを提供する管轄区域との結びつきが弱いか緩やかなOTTサービスを標的とするアクセスへと劇的に移行している。これにより、国際的に事業を展開するサービスプロバイダーが、どのような場合に現地当局にユーザーデータや通信内容を（提供できるべきか）引き渡すべきかという疑問が生じる。関連する考慮事項には、データの所在、対象ユーザー、ユーザーの国籍、調査対象の管轄区域固有の事情などが含まれる。

サービスプロバイダーによる暗号化の導入は、この状況をさらに複雑化する要素である。サービスプロバイダーの観点からは、特定の状況において有効な法的手続きに基づく場合のみユーザーデータを提供できるよう、暗号化手法を設計する必要性が高まっている。より具体的には、暗号化手法はユーザーデータや通信の露出を制限し、政府のアクセス要求への対応複雑性を低減する措置の必須要素となりつつある。エンド・ツー・エンド暗号化は、合法的な政府要求に応じるためのコンテンツデータが提供不能となる結果をもたらす可能性がある。しかし、そのような場合にサービスを遮断することは明らかに不均衡である。

234 参照：Karol Jakubowicz. 初期段階：国連、ICT、表現の自由. 『*国連と表現・情報の自由*』第10章、341頁以降。

235 例：クリスティナ・イリオン『政府クラウドコンピューティングと国家データ主権』2012年6月30日 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1935859また参照：ヨリス・ファン・ホーボケン、アクセル・アーンバック、ニコ・ファン・エイク『雲に隠されたもの、あるいは国外からの政府によるクラウドデータへのアクセスへの対処法』2013年6月9日。http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103。

近年、企業、特にオンライン仲介業者は、人権実施に関する議論の焦点としてますます注目されるようになった。[236] この背景を踏まえると、オンライン仲介業者[237]がコンテンツ提供者とユーザーの間の仲介役であるだけでなく、様々な側面で「セキュリティ仲介業者」としての役割も担っていることに注目する価値がある。暗号化に関する彼らの実践とデフォルト設定は、ユーザーがこれらのテクノロジーにアクセスし効果的に利用する上で極めて重要である。膨大なデータが彼らのルーターを経由しクラウドに保存されるため、諜報機関や非国家アクターにとって理想的なアクセスポイントを提供している。したがって、おそらく意図せずとも、暗号化ポリシーにおいて国家とユーザーの間のインターフェースとして機能しているのだ。この役割は人権議論にも反映されるべきであり、今日の新たなインターネットガバナンスモデルにおいて、ユーザーの情報と通信の安全性を包括的に統合することを求めている。

人権と暗号化：義務と行動の余地

下表は、対処可能な具体的なリスク、関連サービスにおける暗号ソリューションの採用状況、およびこれらのリスクを効果的に対処するための最低要件と優良事例を示す。本調査で特定された人権と暗号ポリシーに関する最低要件は網羅的ではなく、様々なレベルでの実践における規範開発の指針として提示されるものである。

リスク	関連サービスにおいて、暗号ソリューションを採択するために	ベストプラクティス
コンテンツへのアクセスに対する技術的制限（ブロック） 傍受 国家および非国家アクターによるハッキング 通信分析と監視 コンテンツの信頼性や真正性への干渉	クラウドストレージプロバイダー インターネット接続プロバイダー 出版社サイト 検索エンジン メッセンジャー及び通信サービス ブラウザ	公開コンテンツへの安全な認証アクセス 法的確実性 干渉に関する透明性 エンドツーエンドの安全な通信の利用可能性 匿名アクセス機能の有無 教育（メディアリテラシー及び情報リテラシーを含む） 基準と革新

236 参照：国連ビジネスと人権に関する指導原則。2011年。http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf およびユネスコ刊行物『オンライン上の自由の促進。インターネット仲介業者の役割』。2014年。http://unesdoc.unesco.org/images/0023/002311/231162e.pdf。

237 参照：Karol Jakubowicz. 初期段階：国連、ICT、表現の自由. 『国連と表現・情報の自由』第10章、324頁以降。

暗号化手法の使用・展開の自由に対する具体的な干渉事例においては、国際人権基準を踏まえつつ、法的・社会的・技術的状況を考慮した法的評価を行う必要がある。ユネスコが提唱するインターネット普遍性のこのコンセプト、すなわち開放性、万人のアクセス可能性、マルチステークホルダー参加の重視も適用可能である。こうした最低限の要件や優良事例は抽象的な法的分析に基づくものの、評価は具体的状況において行わねばならない。

要約すると、いくつかの事例を挙げて指摘できる。例えば、公開コンテンツへの安全な認証アクセスは、公的・私的検閲の多くの形態に対する防護策となり、改ざんのリスクを制限する。これはオンライン公共圏への信頼、およびオンラインサービスや電子商取引全般への信頼を促進し得る。[238] 安全な認証アクセスを可能にする最も普及した技術標準の一つがTLSである。これと密接に関わるのが、情報への匿名アクセス可能性だ。これによりユーザーは、個人的・政治的関心の分野を問わず、報復を恐れず、あるいは他者への説明責任を負うことなく知識を得られる。前述の通り、TORはオンライン上で実質的に匿名で情報を取得できるシステムである。コンテンツへのアクセスという両側面は、思考と表現の自由に直接寄与する。

法的確実性の原則は、暗号手法や実践に関わるあらゆる司法手続きにおいて不可欠である。法的確実性は結果を予測可能にし、市民が自らの行動をより意識的に形成することを可能にする。したがって、この原則はあらゆる形態の傍受や監視において重要であり、基礎となる法的規範が正確に策定されている場合など、監視に対する不当な懸念を防ぐことができる。ゆえに法的確実性は、人権の行使の抑制要因を減らすことで萎縮効果を回避しうる。

暗号技術分野における継続的な革新と、新たな技術基準の設定・普及も同様に不可欠である。計算能力が絶えず向上するにつれ、暗号規格は急速に陳腐化する。したがって、一定の保護水準を維持することさえ、暗号技術の継続的な近代化とその迅速な普及を必要とする。ここで教育は、これらの規格を確立し普及させる上で重要な役割を担う。なぜなら、情報の暗号化はほとんどの場合、二者以上の当事者による共同作業を必要とするからだ。ユーザー自身も、問題に遅れを取らないよう、継続的なメディアリテラシーと情報リテラシーを必要とする。

制限の合法性

私たちは今、暗号化に関する人権保護の範囲を示した。しかし人権の実際の影響は、国家がこれらの自由に課し得る制限を分析して初めて評価できる。国家安全保障は、言論の自由やプライバシー権を制限する行為の正当な目的となり得る。ただしその措置は必要かつ比例的でなければならない。それが該当するかは、個々の事例ごとに判断される。しかし、この分析は、上述のように表現の自由とプライバシーに保障された権利としての暗号化に対する国家の干渉の合法性を検証する際に、極めて重要な基準となり得る。この権利への干渉は特に以下の場合に深刻である：

- メディア・通信分野における主要サービスプロバイダーが、安全な通信手段を通じてユーザーの情報と通信を保護する能力に影響を与える場合

238 より詳細な議論については、セクション2を参照のこと.

暗号化手法やプロトコルを通じてユーザー情報を保護する能力を損なう場合、ネットワーク通信サービス・テクノロジー利用者に求められる「妨げられない通信」の要件を侵害する。

- 国家は、脆弱なコミュニティやジャーナリストのような構造的に重要な主体が暗号化技術にアクセスする可能性を低下させる。
- 単なる理論上のリスクや危険性が、国家の法制度下における関連する基本的権利の制限を招く場合。
- 国家の行動様式、例えば非公式かつ任意の取り決めを通じて基本権利の制限が確立される場合、導入された暗号化手法・テクノロジーが説明責任のない形で回避・侵食される結果を招く。

6. 提言

一般的な提言

暗号手法はメディア・通信環境の不可欠な要素として認識される必要がある。人権の観点から最終的に重要なのは、暗号手法が情報・通信・コンピューティングにおける人間向けの特性を保護することで、個人のプライバシーと表現の自由の享受を力づける点だ。これらの特性には、情報・通信の機密性、プライバシー、真正性、可用性、完全性、匿名性が含まれる。

人権の観点から、関連する法律や政策手段において暗号化を保護することは特に重要である。なぜなら、暗号化によって、本来は安全でない通信プラットフォームであるインターネット上での情報と通信を保護することが可能になるからである。当初、インターネット自体は、情報と通信の安全性を一般的に提供するように設計されていなかった。長年にわたり、暗号技術はインターネットの中核的構成要素となり、その実践的な実装を支える数多くのプロトコルや標準によって支えられてきた。暗号化は特定の環境において、機密性、プライバシー、真正性、可用性、完全性、匿名性の確保を可能にする。これによりインターネットユーザーの人の権利、特に表現の自由とプライバシーの保護が促進される。

暗号化と人権に関連する構造的条件に関するさらなる提言を以下に示す：

[1] 暗号化ポリシーは、インターネットガバナンスのより広い文脈、およびインターネットの様々な利用が関わるより広範な社会的機能や人間の価値観の中で捉えられるべきだ。

[2] 暗号化ポリシーに関する議論において、人権の視点の代表性を強化しなければならない。実際には、国家安全保障や経済競争力などの他の考慮事項が支配的な要因となる傾向があるものの、人権の視点の代表性を高めるには以下が必要である：

- 人権基準と国際規範形成に対するより強固な認識；

- 干渉に対する保護策の構築、ならびに国家・産業関係者及びユーザーによる良き慣行の確立；
- 暗号化プロトコルや実装に対する非合法的な干渉（非公式な「バックドア」、標準設定などを含む）からの保護の必要性、およびメディア・通信環境における信頼の構築；
- メディア・通信のセキュリティに対する非公式な非法的干渉に関する透明性要件；
- プライバシーとセキュリティを保証するテクノロジーを導入する際の、透明性のあるソフトウェア実施基準と説明責任の促進；
- 女性と女子、その他オンライン上の脆弱なグループ（民族的・人種的少数派、LGBTコミュニティを含む）の権利侵害における暗号化の役割への配慮；

[3] すべての関連する利害関係者が関与すべきである。この問題は政府や産業界だけでなく、市民社会の構成員、少数派、女性と女子を含む脆弱なコミュニティの代表者、メディアや教育機関も含まれるべきである。

[4] 暗号化が人権保護の万能薬ではないことを認識すべきだ。効果を発揮するには、他の人権支援や保護策と組み合わせて運用する必要がある。

ステークホルダーへの提言

本調査で示された考察は、様々なステークホルダーにとって有用な知見をもたらす。以下の提言は、人権問題と公共の安全・セキュリティなどの正当な考慮事項との適切な均衡を図るための検討事項である。各提言は異なるステークホルダーグループ（ユーザー、サービスプロバイダー、テクノロジー専門家、立法者）と、彼らがシステム全体で担う特定の役割を対象としている。

国家が考慮すべき事項：

[5] ユーザー及び関連サービスプロバイダーによる暗号化技術の導入に対して、一般的な制限を課すことを控えること。

[6] 関連分野全体の暗号化ポリシーに人権を考慮し、暗号化ポリシーがジェンダーに配慮するとともに、保護対象となる少数派の特定のニーズにも応えることを確保すること。

[7] 法的確実性の確立 – 法的確実性の欠如は、市民も業界関係者もリスクを適切に評価できないため、特に自由で開かれたコミュニケーションを阻害する可能性がある；

[8] 透明性の確保－特に政府と業界関係者間の非公式合意は、暗号化分野における人権リスクを引き起こす可能性がある。これは政府への行為帰属を阻害し、人権を効果的に適用するための前提条件を損なうからである；

[9] 政府による合法的なアクセスに関するポリシー立案を、恐怖に基づくものではなく事実に基づくものとし、関連する全てのコミュニティをこの質問に関与させること；

[10] 暗号化ポリシー問題における国際的な連携強化に取り組むこと；

[11] メディア・通信環境における暗号技術の革新と標準化に関する研究開発を促進すること；

[12] ユーザーの通信と情報を保護するテクノロジーの採択（及びその欠如）を評価するためのグローバルな監視・測定スキームを開発すること；

[13] ユネスコの「インターネットの普遍性と知識」というコンセプトを考慮すること。これには、暗号化への制限がインターネット上の人権、開放性、全ての者へのアクセス性に与える影響を議論するためのマルチステークホルダープロセスを含む。

民間セクターとインターネット仲介業者は以下を検討できる：

[14] オンライン仲介業者は、コンテンツ提供者とユーザーの間の仲介業者であるだけでなく、様々な側面において「セキュリティ仲介業者」として認識されるものとする。

[15] 通信のエンドツーエンド暗号化や保存データの認証付き暗号化など、ユーザーのプライバシーと表現の自由の確立・促進に寄与するあらゆる適切なセキュリティ対策を継続的に導入すること。

[16] ユーザーが享受する保護水準において「最低水準への競争」ではなく「最高水準への競争」を促進する形で、国際的かつ管轄区域を越えた取り組みを行うこと。

[17] ユーザーのプライバシーと表現の自由を保護するため、暗号技術の導入において革新を図る。

[18] プライバシー強化テクノロジーと人権指向の暗号化プロジェクトのオープンな開発を支援すること；

[19] 安全なコーディング慣行を促進し、サービスにおける機密性と匿名性の向上に向けた取り組みを強化する。

[20] ソフトウェアエコシステムにおける分断化課題に対処するため、標準化への調整と貢献の努力を強化すること[239]

ユーザー、市民社会、技術コミュニティは以下を検討できる：

多くの国での調査は、相当数のユーザーがプライバシー問題を重要視していることを示している。その結果、個人や職業上のオンラインサービスのプライバシーに対する信頼が裏切られたと知ると、彼らは不満を抱き、時には敵意すら示す。しかし、大多数のユーザーは利用可能な暗号化手段を用いてプライバシー強化に投資しない可能性がある。研究によれば、これはユーザーがプライバシーに価値を置いていないというよりも、諦めの表れと理解すべきである。

239 バークマン・センター2016年報告書（「ソフトウェア・エコシステムは断片化しがちである。暗号化技術が広く普及し包括的になるためには、現 状 よりもはるかに高度な調整と標準化が必要となる」）を参照のこと。

この指摘された乖離は、暗号テクノロジーだけでなく他のプライバシー保護手段においても観察される。この観点から、私たちはこの後のアプローチを推奨する：

[21] プライバシー保護は、暗号テクノロジーを利用するユーザーだけに依存すべきではない。リスクの周知とテクノロジー知識の普及は国家ポリシーの一環とすべきであり、ジャーナリスト、女性と女子、少数派など様々な脆弱性を持つグループを含む全ユーザーへの啓発に十分な配慮が必要だ。各国は暗号化リテラシーを、コミュニケーション・メディア・情報リテラシープログラムに組み込むよう促されるべきである。これらの措置の効果は限定的かもしれないが、情報に基づいたユーザーを中心に据えるポリシーにおいて重要な要素であり続ける。

[22] 暗号化を可能な限り便利にするスマートテクノロジーは、ジャーナリスト、メディア関係者、女性と女子、少数派といった脆弱なユーザー（例えば、特別な保護措置）を含め、プライバシーと表現の自由を支える。より高いレベルの暗号化が必要な状況を認識し、その要求に自動的に対応するシステムは有用だろう。ユーザーは通信のセキュリティについて繰り返し判断したくないかもしれないが、デバイスやソフトウェアシステムを選択する際に一度だけ判断することは可能だ。

[23] 消費者の利益が関わる場合、個々のユーザーに依存するだけでなく、消費者利益を保護する機関を強化することが効果的かもしれない。

[24] プライバシーポリシーは、通信や取引においてユーザーにサービスを提供する仲介業者を対象とすべきだ。このレベルで効果的な暗号化が実現されていれば、リスクを認識していないユーザーさえも保護される。

[25] 教育と訓練には重要な役割があり、より一般的な目標として、人々が行うべきことは、直面するリスクについて現実的な認識を持ちつつ、コンテンツや通信への不正アクセスから自らを守るという不可能な要件に煩わされないようにすることです。この目的のための取り組みは、暗号化が利用されない理由に関する研究に基づいて構築できる。[240]

[26] ジェンダーの側面と脆弱なコミュニティ：女性と女子、ジャーナリスト、メディア関係者、保護対象の少数派といった脆弱なコミュニティは、人権侵害にさらされやすく、暗号化通信をより必要としている。彼らの問題に対する特別な強化策が求められる。

[27] 人権に関する議論は、テクノロジーコミュニティが提供する専門知識から大きな恩恵を受け得る。したがってテクノロジー専門家の関与は歓迎されるべきだ。テクノロジー専門家は自らの決定がプライバシーと通信の自由に及ぼす影響を考慮すべきである。こうした配慮は職業倫理と研修に反映される必要がある。

[28] 技術基準における人権促進を目的とした、マルチステークホルダー基盤の標準設定コミュニティプロセスは支援され、さらに強化されるべきだ。既知の脆弱性を持つプロトコルの迅速な改善に向けた取り組みを優先すべきである。

240 例：K. Renaud、M. Volkamer、A. Renkema-Padmos。

参考文献

Harold Abelson et al., Keys Under Doormats: 政府がすべてのデータと通信にアクセスすることを要件として、不確実性を強制する、July 2015, http://www.crypto.com/papers/ Keys_Under_Doormats_FINAL.pdf.

アクセス・アンド・ペン・アメリカ人・センター、暗号化／匿名性に関するコメント、国連への提出文書、2015年。

Bhairav Acharya,『インドの暗号化ポリシー短命な冒険』, 2015年12月, https://www.ocf.berkeley.edu/~bipla/the-short-lived-adventure-of-indias-encryption-policy/.

ACLU、スティングレイ追跡デバイス：誰が所有しているのか？、https://www.aclu.org/map/stingray-tracking-devices-whos-got-them（最終アクセス：2016年8月29日）。

ベン・アディダ他、CALEA II：エンドポイントへの盗聴改造のリスク、民主主義＆テクノロジーセンター、2013年5月17日、https://www.cdt.org/files/pdfs/ CALEAII-techreport.pdf（最終アクセス：2016年9月14日）。

マリオン・アルバース、『情報自己決定権』、バーデン＝バーデン、2005年。

ロバート・アレクシー、ジュリアン・リバース著『憲法上の権利の理論』、オックスフォード、2010年。

アプッツォ他、「Apple他テック企業がデータアクセスを巡り米国と対立」、ニューヨーク・タイムズ、2015年9月7日。

アクセル・アーンバック『*私的通信の保護：EU法における私的通信の安全保障*』*E.U.法における私的通信の保護：基本的人権、機能的バリューチェーン、市場インセンティブ*、クルワー・ロー・インターナショナル、2016年。

キム・アローラ、「国家暗号化ポリシー草案がオンラインで公開され、専門家が懸念を示す」、『タイムズ・オブ・インディア』、2015年9月20日。

Aydin 他、トルコ対暗号化：表現の自由への攻撃、Access、2015年9月[3日]。

ジャック・バルキン、「デジタル言論と民主主義文化：情報社会における表現の自由の理論」、NYU Law Review 79 (2004)。

デレク・バンバウアー、『オーウェルの肘掛け椅子』、『シカゴ大学ロー・レビュー』79号（2012年）、3頁、pp. 863-944頁。

BBC、MI5長官がテクノロジーテロのリスクを警告、BBC UK、2015年9月17日。

コーリー・ベネット、ケイティ・ボー・ウィリアムズ、「パリ、政府による暗号化データへのアクセスをめぐる争いを再燃させる」、ザ・ヒル、2015年11月17日。

バークレー情報プライバシー法協会ブログ、インドの暗号化ポリシー短命な冒険。

バークマン・センター、「慌てるな：『暗闇化』論争の進展」、2016年2月1日。ダニエル・バーンスタイン、タン

ジャ・ランゲ、ルーベン・ニーダーハーゲン、「デュアル EC：標準化されたバックドア」。暗号学電子印刷アーカイブ：レポート 2015/767。

BITKOM調査 08/2014 サイバー犯罪、https://www.bitkom.org/Presse/Anhaenge-an-PIs/2014/ August/140827-BITKOM-Charts-PK-Cybercrime-mit-BKA-28-07-14.pdf。

トーマス・ベッケンフェルデ、電子的プライバシーへの道、JZ 2008、pp. 925-939。マルクス・ベーム、メッセンジャー

Telegram：ISテロリストのお気に入りアプリがプロパガンダチャンネルを閉鎖、2015年11月18日、http://www.spiegel.de/netzwelt/apps/is-auf-Telegram-messenger-アプリが措置を予告している-a-1063535.html。

ガブリエレ・ブリッツ、情報技術システムの機密性と完全性、DÖV 2008、pp. 411-414頁。

ベルナール・カズヌーヴ、フランス内務大臣、トーマス・ド・マイジエール、ドイツ内務大臣との共同記者大会における演説、パリ、2016年8月23日、http://www.interieur.gouv.fr/Le-ministre/Interventions-du-ministre/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe（2016年9月14日最終アクセス）。

Citizen Lab（トロント大学ムンク国際問題大学院）およびコリン・アンダーソン、「表現の自由の権利を確保するためのデジタルセキュリティソリューションの民主化の必要性」、意見と表現の自由の権利の促進と保護に関する特別報告者、デビッド・ケイ氏への共同提出文書、2015年2月10日 http://www.ohchr.org/Documents/Issues/Opinion/Communications/CitizenLab.pdf。

ジェームズ・コミー、「暗闇へ：テクノロジー、プライバシー、公共の安全は衝突コースにあるのか？」 2014年10月、ブルッキングス研究所でのスピーチ、https://www.fbi.gov/news/speeches/ going-dark-are-technology-privacy-and-public-safety-on-a-collision-course。

CTITF、『テロ目的でのインターネット利用対策－法的・技術的側面』、ワーキンググループ総覧（2011年5月）。

マイケル・チェルトフとトビー・サイモン、「ダークウェブがインターネットガバナンスとサイバーセキュリティに与える影響」、グローバル・インターネットガバナンス委員会論文シリーズ：第6号（チャタムハウス、2015年2月）

欧州評議会研究部、国家安全保障と欧州判例法、欧州評議会／欧州人権裁判所、2013年。

欧州評議会議会、法務・人権委員会、報告者：ピーター・オムツィクト氏、2015年3月18日付「大量監視に関する報告書」、文書番号13288。

ジョセフ・コックス、AppleのiMessageによるスパイ対策には欠陥がある、Wired、2015年9月8日、http://www.wired.com/2015/09/apple-fighting-privacy-imessage-still-problems/。

ライアン・カロ、政府の監視に抵抗する最良の希望はテクノロジー企業かもしれない、フュージョン、2015年9月7日。

ケインズ＝ローン、ブランディス／ドルフ、マイケル・C.、「萎縮効果の測定」、NYU Law Review 90 (2015)、pp. 1095-1114。

コナー＝サイモンズ、CSAIL報告書：政府にデータへの特別アクセス権を与えることは重大なセキュリティリスクをもたらす、MITニュース、2015年7月7日。

インドデータセキュリティ評議会およびNASSCOM、暗号化ポリシーに関する提言。

ローラ・デナルディス、インターネットの管理する手段の隠れた側面、情報・コミュニケーション・社会 pp. 37-41, 2012.

クラウディア・ディアス、オマー・テネ、セダ・ギュルセス、「英雄か悪役か：プライバシー法とテクノロジーにおけるデータ管理者」、74 (2013) オハイオ州法ジャーナル、pp. 923-964。

エコノミスト誌、TSAは締め出された、2015年9月19日。

EFF、匿名性と暗号化、国連意見及び表現の自由の権利の促進と保護に関する特別報告者への意見書、2015年2月10日。

EFF,『EFFのウェブ暗号化レポート』, 2014年11月, https://www.eff.org/encrypt-the-web-report.

EFF. セキュアメッセージング評価表、2015年11月3日版、https://www.eff.org/secure-messaging-scorecard。

ENISA および ユーロポール。21 世紀のデータ保護を尊重する合法的な犯罪捜査について。ユーロポール および ENISA 共同声明。2016 年 5 月 20 日。

マーティン・アイファート、インターネットにおける情報に関する自己決定権。Das BVerfG und die Online-Durchsuchungen、NVwZ 2008、521-523 ページ。

EPIC、デジタル通信における暗号化と匿名性の使用、国連への提出文書、2015年2月10日。

EPRS、科学技術オプション評価（STOA）、大量監視、第 1 部 - 現在の世代のネットワークサービスおよびアプリケーションによって生じるリスクと機会、2014 年。

EPRS、科学技術オプション評価（STOA）、大量監視、第2部ーテクノロジー予測、長期的なセキュリティとプライバシー向上のための選択肢、2014年。

欧州議会決議、2015年9月8日、「人権とテクノロジー：第三国における人権への侵入・監視システムの影響」、2014/2232(INI)［マリエチェ・シャーケ報告者］。

ユーロポール、インターネット組織犯罪脅威評価（IOCTA）2015、2015 年 9 月 30 日、オンライン版は https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 で閲覧可能（最終アクセス日：2016年9月14日）。

エド・フェルテン、「セキュリティ・バックドアについて」、Freedom to Tinker、2013年9月11日、https://freedom-to-tinker.com/blog/felten/on-security-backdoors/。

エド・フェルテン、「ソフトウェアのバックドアとホワイトハウスNSAパネル報告書」、Freedom to Tinker、2013年12月、https://freedom-to-tinker.com/blog/felten/software-backdoors-and-the-white-house-nsa-panel-report/。

クリスティン・フィンクレア、ダークウェブ、CRS報告書、2015年7月7日。

ジム・フィンクル、香港デモ参加者を標的とした高度なiOSウイルス - セキュリティ企業、ボストン、2014年9月、http://www.reuters.com/article/hongkong-china-cybersecurity-apple-idUSL2N0RV2D320140930。

FOSS、暗号技術は公共の利益にとって重要だ、2015年。

トム・フォックス＝ブリュースター、「Facebook、匿名Torユーザー向けに.onionアドレスを提供開始」、ガーディアン、2014年10月31日、http://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users-onion。

チャールズ・フリード、「プライバシー」、イェール・ロー・ジャーナル 77 (1968)、pp. 475-493。

ケビン・ギャラガー、「なぜより多くの報道機関がSTARTTLS暗号化でメールを保護しないのか？」、2015年2月24日、https://freedom.press/blog/2015/02/why-arent-more-news-organizations-protecting-e-mail-with-starttls。

エリック・ゲラー、「新たな『暗号戦争』完全ガイド」、The Daily Dot、2016年4月26日。http://www.dailydot.com/politics/encryption-crypto-wars-backdoors-timeline-security-privacy/ で閲覧可能。

ユリア・ゲルハルトス、『暗号化への（基本的）権利？』、バーデン＝バーデン、2010年。

サミュエル・ギブス、「検察官によると、Googleは一部のAndroidデバイス（遠隔ロック解除可能）を、もしデバイス未暗号化である場合」ガーディアン、2015年11月24日、http://www.theguardian.com/technology/2015/nov/24/google-can-unlock-android-devices-remotely-if-phone-unencrypted。

アンディ・グリーンバーグ、警察はiPhoneに侵入するために暗号化のバックドアを必要としない、2015年10月12日、http://www.wired.com/2015/10/cops-dont-need-encryption-backdoor-to-hack-iphones/。

Graham Greenleaf, 世界のデータプライバシー法 2015：109カ国、欧州の法律は今や少数派、133*件のプライバシー法とビジネス国際報告書*、2015年2月。

GNI、国連への提出文書、2015年。

Peter Gola & Rudolf Schomerus, 『連邦データ保護法』第12版、ミュンヘン、2015年。Dan Goodin, 「低コストのIMSIキャッチャーが4G/LTEネットワークで携帯電話の正確な位置を追跡」、アーストゥルニカ、2015年10月28日、http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/。

ジェニファー・グラニック、「暗闇化」論争に連邦判事がスポットライトを当てる、インターネット・社会センター、2015年10月、http://cyberlaw.stanford.edu/blog/2015/10/federal-judge-shines-spotlight-%E2%80%9Cgoing-dark%E2%80%9D-debate。

アパール・グプタ、「何ビットで十分か？暗号化の合法性」、2011年11月、http://www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/。

セダ・ギュルセスとバート・プレネル、「暗号学とプライバシー」、ヴァン・デル・スルート、ブルードゥース、シュライバース（編）、*『ビッグデータの境界を探る』*、オランダ政府政策科学評議会、2016年。

ヘニンガーとハルダーマン、「暗号コミュニティからの物語：NSAはサイバーセキュリティを損なった。今こそ真実を明らかにすべきだ、フォーリン・アフェアーズ、2013年10月23日。

ライアン・ヘンリー、ステイシー・ペティジョン、エリン・ヨーク著『国務省インターネット自由プログラムのポートフォリオ評価』ランド国家セキュリティリサーチ部門、2014年2月、http://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1035/ RAND_WR1035.pdf。

マティアス・ヘルデゲン著『国際法』第14版、ミュンヘン、2014年。

アレックス・ハーン、「ハッキングチームがハッキング被害：抑圧的な政権にスパイツールを販売していたと文書が主張」、ガーディアン、2015年7月、http://www.theguardian.com/technology/2015/jul/06/ hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim。

ヨリス・ファン・ホーボーケン、アクセル・アーンバック、ニコ・ファン・エイク『雲に隠されたもの、あるいは国外からの政府によるクラウドデータへのアクセスへの対処法』2013年6月9日、http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103。

トーマス・ホーレン、ウルリッヒ・ジーバー著『マルチメディア法ハンドブック』、ミュンヘン、2012年。

ヴォルフガング・ホフマン＝リーム著『機密性および情報技術システムの完全性の保障に関する基本権』、JZ 2008年、1009-1022頁。
情報技術システムの完全性に関する基本権、JZ 2008年、pp. 1009-1022。

ジャンネット・ホフマン、「インターネットガバナンスにおける信頼と不信の構図」、『専門家グループ報告書「信頼の浸食リスクー欧州研究・イノベーションポリシーへの中期的影響に関する先見性（TRUSTFORESIGHT）」』、欧州委員会、ブリュッセル、2015年。

ゲリット・ホーヌング、「暗号論争：不死者の帰還」、MMR 2015、145-146頁。ゲリット・ホーヌング、「新たな基本権」、CR 2008、299-306頁。

Human Rights Watch＆ACLU、『監視の自由：大規模な私たち米国監視がジャーナリズム、法律、そしてアメリカ人の民主主義に与える危害』（2014年）。

インド法とテクノロジーブログ、何ビットで十分か？暗号化の合法性、インド法とテクノロジーブログ、2011年11月 http://www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/。

インド電気通信法・規制ハンドブック、2013年。第1巻。

1999年インド国家電気通信ポリシー、http://www.dot.gov.in/telecom-polices/new-telecom-policy-1999。

2012年インド国家通信ポリシー、http://www.dot.gov.in/sites/default/files/NTP-06.06.2012-final.pdf。

インド政府ポリシー草案、2015年9月、http://www.scribd.com/doc/282239916/ DRAFT-NATIONAL-ENCRYPTION-POLICY。

クリスティナ・アイリオン、政府クラウドコンピューティングと国家データ主権、2012年6月30日、http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1935859。

インセラ他『暗号化と法執行機関の特別アクセス：米国はより強力な暗号化を優先すべき』ヘリテージ財団、2015年。

International Journal of Computer Application,「インドにおける暗号技術に関連する法的問題」.インターネットアーキテクチャ

委員会（IAB）,「広範な監視下における機密性：脅威モデルと問題定義」, 2015年8月, http://tools.ietf.org/html/rfc7624. モデルと問題定義、2015年8月、http://tools.ietf.org/html/rfc7624。

サラ・ジョセフ、メリッサ・カスタニョ著『市民的及び政治的権利に関する国際規約』第3版、オックスフォード、2013年。

デイヴィッド・ケイ、電話暗号化：プライバシーと保護のバランス、NYTimes 編集者への手紙、2015年8月21日。

デイヴィッド・ケイ、意見及び表現の自由の権利の促進及び保護に関する特別報告者の報告書、2015年5月、http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc。

エリック・キングとMatthew・ライス、「時代遅れ：英国はいつIMSIキャッチャーが存在しないふりをやめるのか？」、2014年11月、https://www.privacyinternational.org/node/454。

ナディム・コベイシ、暗号化とテロリストについて、2015年11月23日。

ニール・コブリッツとアルフレッド・メネゼス、「謎に包まれた謎」、2015年12月、http:// eprint.iacr.org/2015/1018.pdf。

アレクサンダー・コッホ、「暗号化の権利？」、CR 1997、106-110 ページ。

Eitan Konigsburg、HTTPS の採用、2014 年 11 月、http://open.blogs.nytimes. com/2014/11/13/embracing-https/。

Bert-Jaap Koops、暗号法の調査 - 国別概要 - バージョン 27.0、2013 年 2 月。Joshua Kopstein、FBI 長官、テクノロジー企業にエンド・ツー・エンド暗号化の提供中止をする、2015年 12 月 9 日 2015年12月9日、http://motherboard.vice.com/read/fbi-chief-has-tech-companies-stop-offering-end-to-end-encryption.

クリストファー・クーナー、2013年。

クリストファー・クーナー、私たち暗号戦争に実際に敗北した、LSEメディアポリシープロジェクト、2014年11月12日、http://blogs.lse.ac.uk/mediapolicyproject/2014/11/12/we-actually-lost-the-crypto-wars/。

マイカ・リー、Appleは依然として連邦当局に提供できるあなたのデータの大量を保有している、The Intercept、2014年9月22日、https://theintercept.com/2014/09/22/apple-data/.

Julian von Lucius, GMailはTKGの定義における電気通信サービスである, 2015年12月11日, http://www.noerr.com/de/presse-publikationen/News/gmail-ist-ein-telekommunikationsdienst-im-sinne-des-tkg.aspx.

ジョナサン・マーラー、誰があの誹謗中傷を吐いたのか？ 匿名アプリ「Yik Yak」は明かさない、ニューヨーク・タイムズ、2015年3月8日。

レベッカ・マッキノン他、『オンライン上の自由を育む：インターネット仲介業者の役割』、ユネスコ／インターネット協会、2014年。

マコーネル、チェルトフ他、「遍在するデータ暗号化への懸念が誇張されている理由」、論説、ワシントン・ポスト、2015年7月28日。

キーラン・マッカーシー、オランダ政府はバックドアを拒否、目をそらさずにOpenSSLに54万ドルを投入、ザ・レジスター、2016年1月4日。

ドミニク・マクゴールドリック『人権委員会』クラレンドン・プレス、1994年。

ターラック・マクゴナグル、イヴォンヌ・ドンダース著『国連と表現の自由・情報の自由』ケンブリッジ大学出版局、2015年。

マクスウィーニー、あなたのデータのセキュリティが心配か？暗号化が個人情報を守る方法、ハフポスト、2015年9月3日。

アミール・ミズロック、「監視とシリコンバレーが欧州のプライバシー均衡を『破壊』している」。2015年12月11日。http://blogs.wsj.com/digits/2015/12/11/surveillance-silicon-valley-destroying-europes-privacy-balance。

ピーター・ミュンヒ、『技術的・組織的データ保護』、第4版、フレッヒェン、2010年。

エレン・ナカシマ、FBI長官：テログループが暗号化通信に依存、ワシントン・ポスト、2015年7月8日。

エレン・ナカシマ、オバマ大統領、広範な暗号化支援への機運の高まりに直面、ワシントン・ポスト、2015年9月16日。

マイケル・ネルソン、クリントン、クリッパー、暗号、ザ・ヒル、2015年9月10日。

ヘレン・ニッセンバウム、「コンピュータセキュリティと国家安全保障の接点」、*『倫理と情報テクノロジー』*第7号（2005年）、61-73頁。

マンフレッド・ノヴァク、『CCPR解説』、第2版、2005年。

国家安全保障会議（NSC）暗号化戦略アプローチに関する草案オプション論文、2015年夏、http://apps.washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches-to-encryption/1742/。

OECD、暗号ポリシー、ガイドラインと課題、1998年。

A. パルヴァティ、ラヴィ・シャンカール・チョードリー、ヴリジェンドラ・シン『インドにおける暗号技術に関連する法的問題』2013年4月、International Journal of Computer Application、第2巻第3号、http://rspublication.com/ijca/april13/6.pdf。

Andrea Peterson,「ワシントン・ポスト紙、訪問者向けにウェブサイトの一部を自動暗号化開始」, WaPo, 2015年6月30日.

アンドレアス・フィッツマン、『技術によるデータ保護』、DuD 1999年、pp. 405-408。アンドレアス

・フィッツマンとマリット・ハンセン、『匿名性、非関連性、非観測性、仮名性、およびアイデンティティ管理 — 用語体系に関する統合提案」、バージョン v0.25、2005年12月6日。

イェルク・ポーレ、「設計段階でのデータ保護の失敗：その短史」、FIfF-Kommunikation 2/15、pp. 41-44。

イザベル・ド・ポムロー『スノーデンの後、暗号スタートアップがドイツに根付く』CSモニター、2015年8月3日、http://www.csmonitor.com/World/Passcode/2015/0803/In-Snowden-s-wake-crypto-startups-take-root-in-Germany。

Privacy International、Article 19 & IHRC、『オンライン上の安全な空間の確保』、2015年。

Privacy International、国連表現の自由特別報告者への提出文書 – デジタル通信における匿名性と暗号化、2015年2月。

パブリック・インテリジェンス、インド国家暗号化ポリシー草案、2015年9月。

ナンダゴパル・ラジャン、暗号化ポリシー：抗議を受けてWhatsAppとウェブサービスが暗号化ポリシー草案から除外、2015年9月、http://indianexpress.com/article/technology/tech-news-technology/draft-national-encryption-policy-you-might-need-to-store-whatsapp-messages-for-90-days/。

OECD、暗号ポリシーに関するOECDガイドライン、1997年3月27日。

P. リーガン、『プライバシーの立法化：テクノロジー、社会的価値、公共ポリシー』、チャペルヒル：ノースカロライナ大学出版局、1995年。

Philipp Rogaway、暗号化の道徳的性格、カリフォルニア大学、2015年12月。

サーシャ・ロマノスキー、マーティン・C・リビッキ、ゼブ・ウィンケルマン、オレシア・トカチェバ、『インターネットの自由ソフトウェアと違法行為、犯罪者を支援することなく人権を支援する』、ランド社、2015年。

Philipp Roos、Das IT-Sicherheitsgesetz、MMR 2015、636-645 ページ。Alexander Roßnagel、Das

De-Mail-Gesetz、NJW 2011、1473-1478 ページ。

Alexander Roßnagel、情報技術システムのセキュリティ強化に関する法案（IT セキュリティ法）に関する書面による意見、ドイツ連邦議会、内務委員会、委員会印刷物 18(4)(284)B。

Ira Rubinstein および Joris van Hoboken、クラウドにおけるプライバシーとセキュリティ、Maine Law Review 2014、488-533 ページ。

Ira Rubinstein および Michael Hintze、暗号化ソフトウェアの輸出管理する、http://encryption_policy.tripod.com/us/rubinstein_1200_software.htm。

ファビアン・シェルシェル、「WhatsAppの暗号化を監視する」、c't、2015年4月30日、http://m.heise.de/ct/artikel/Keeping-Tabs-on-WhatsApp-s-Encryption-2630361.html。

ステファニー・シーダーマイアー『個人の保護を国際的基本権として』テュービンゲン、2012年。

ブルース・シュナイアー、「私たちインターネットの巨人たちに魂を売り渡した方法」、2015年5月、https://www.schneier.com/essays/archives/2015/05/how_we_sold_our_soul.html。

セバスチャン・シュルツ、『プライバシー・バイ・デザイン』、CR 2012、pp. 204-208。

スピロス・シミティス、『連邦データ保護法』、第8版、バーデン＝バーデン、2014年。

クリス・ソゴイアン、クラウドに囚われて：ウェブ2.0時代のプライバシー、暗号化、政府のバックドア。8 J. on Telecomm. and High Tech. Law 359 (2009)。

Oliver Stiemerling と Jürgen Hartung,「データ保護と暗号化」, CR 2012, pp. 60-68.Thomas Stögmüller,「企業における情報技術システムの機密性と完全性」, CR 2008, pp. 435-439.
企業における情報技術システムの機密性と完全性、CR 2008、pp. 435-439。

ピーター・スワイア、上院司法委員会公聴会「暗闇へ：暗号化、テクノロジー、そして公共の安全とプライバシーのバランス」、2015年7月8日。

ピーター・スワイア、暗号化とグローバル化、コロンビア科学テクノロジー法レビュー、第23巻、2012年、
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602。

ユルゲン・テーガー、デトレフ・ゲーベル著『BDSGおよびTKG・TMGのデータ保護規定』第2版、ノルトシュトラント、2013年。

ポール・テイラー、「スパイを不安にさせるセキュリティ」、フィナンシャル・タイムズ、2010年8月2日、
http://www.ft.com/intl/cms/s/0/7ad48c10-9e5d-11df-a5a4-00144feab49a.html#axzz3R5nCIW6l。

インド電気通信規制庁、アプリケーションサービスに関する勧告。

インド電気通信規制庁、モバイル金融サービスに関するTRAI協議論文。インディアン・エクスプレス紙、バックドアなしの明確で堅牢な暗号化ポリシーが必要だ。

インターネット協会、暗号化に関する声明、2013年11月23日。

インド準備銀行、電子銀行ワーキンググループ報告書。

インド準備銀行、情報セキュリティ、電子銀行業務、テクノロジーリスク管理及びサイバー詐欺に関するガイドライン。

トーマス他、監視法への支持を求めるメイ首相、2015年9月16日、フィナンシャル・タイムズ。

UCI法国際司法クリニック、選定参考文献：暗号化、匿名性及び表現の自由に関する特別報告者報告書（A/HRC/29/32）非公式補足資料、2015年。

ユネスコ、包摂的な知識社会を育むための基幹要素、パリ 2015年、
http://unesdoc.unesco.org/images/0023/002325/232563E.pdf。

国連テロ対策実施タスクフォース（CTITF）、『テロ目的でのインターネット利用対策』、CTITFワーキンググループ報告書（2009年2月）。

私たち米国商務省（産業社会局）『暗号化輸出管理する：ライセンス例外 ENC および大衆市場適格性の改訂』

ヴァンス他、「電話の暗号化が司法を妨げる場合」、NYTImes、オピニオンページ、2015年8月11日。

Andreas Voßhoff および Peter Büttgen、Verschlüsselung tut Not、ZRP 2014、232-235 ページ。W3C、エンドツーエンド暗号化とウェブ、W3C TAG 調査結果 2015年7月16日。

ベン・ワグナー、「アラブの春の後：欧州の外交政策における人権とインターネットの新たな道」、欧州議会、対外政策総局、ポリシー部門、2012年。

ジェーン・ウェイクフィールド、「ISはどのように安全に通信しているのか？」、BBCニュース、テクノロジー、2015年11月17日。

ファビアン・ヴァリスローナー、「タトルト：暗号化。パリ事件後の責任問題」、2015年11月19日、
https://netzpolitik.org/2015/tatort-verschluesselungstechnik-die-schuldfrage-nach-paris。

ニコラス・ウィーバー、「私たちはこの暗号化がテロリストの隠れ蓑になると考えている。そうではない」、2015年12月、https://www.washingtonpost.com/news/in-theory/wp/2015/12/14/we-think-encryption-allows-terrorists-to-hide-it-doesnt。

ダニエル・ワイツナー、「パリ事件後の暗号化解決策はシリコンバレーではなくワシントンから来るべきだ」、ワシントン・ポスト、2015年11月24日。

WhatsApp, WhatsApp暗号化概要, 技術ホワイトペーパー, 2016年4月4日.

トム・ホワイトヘッド、『新法でインターネット企業は破れない暗号化を提供できなくなる』『テレグラフ』2015年11月2日。

ホワイトハウス、国家安保会議、『暗号化への戦略的アプローチの見直し』、リークされた草案メモ、2015年9月、ワシントン・ポスト経由で入手可能。

ザック・Whittaker、カザフスタンは市民にインターネットのバックドア設置を強制する、ZDNet、2015年12月3日。

S・E・ウィルボーン、「公的/私的の区別を再考する」、ジョージア・ロー・レビュー 32 (1998)、825-858 ページ。

ウィルソン・センター・シンポジウム、「私たちはどう変化したか？安全保障と自由に関する米国の見解の変遷」。ボブ・リットの発言、https://www.youtube.com/watch?list=PLzM1iiQhVrdHHZPSZ1z_ztTrUuRPMUtRb&v=PWj8eqKKB64。

ウィッツ、暗号化とゴーイング・ダークに関する考察：パート I、Lawfare、2015 年 7 月 9 日。ウィッツ

ツ、暗号化とゴーイング・ダークに関する考察：パート II、Lawfare、2015 年 7 月 12 日。

World Wide Web Foundation 他、表現の自由、暗号化、匿名性：市民社会と民間セクターの認識、2015年。

Yulong Zou、Xianbin Wang、Lajos Hanzo、無線セキュリティに関する調査：技術的課題、最近の進展、将来の動向、IEEE論文集、2015年5月、http:// arxiv.org/pdf/1505.07919.pdf。

付録1：ユネスコ「点と点をつなぐ」成果文書

成果文書

2015年3月3日～4日にユネスコ本部で開催された「CONNECTing the Dots：将来の行動のための選択肢」大会は、

インターネットが包括的な知識社会に向けた人類の進歩を促進する可能性、及び広範な関係者のエコシステムにおいてこの発展を促進するユネスコの重要な役割を*認識した*。

ユネスコのインターネット関連問題への取り組みの基盤となる人権原則*を再確認した*。具体的には、人権理事会決議A/HRC/RES/26/13に基づき、オフラインで人々がある権利はオンラインでも同様に保護されなければならない。

第37回大会決議52を*想起する*。同決議は、情報社会世界サミットに関するユネスコの取り組み枠組み内で、加盟国が検討するための選択肢を含む協議型マルチステークホルダー研究を実施し、第38回大会に報告することを義務付けた。

さらに、世界人権宣言第12条及び第19条、並びに市民的及び政治的権利に関する国際規約第17条及び第19条を含む指針文書における原則の確立を*想起する*。

また、ユネスコ諮問研究の草案を*レビューした上で*、

以下の関連選択肢に関する継続的な取り組みを*称賛し*、ユネスコ加盟国による審議を期待する：

1. ユネスコのための包括的選択肢

1.1 第37回総会で承認された第1回WSIS+10大会の最終声明を考慮し、インターネットガバナンスフォーラム（IGF）を含む情報社会世界サミット（WSIS）の成果が、ポスト2015開発アジェンダ、インターネットガバナンス問題、及びユネスコの役割と活動にとって継続的な価値を持つことを確認する。

1.2 意見及び表現の自由、その帰結としての報道の自由及び情報へのアクセス権、平和的集会の権利、プライバシーの権利といった基本的権利が、ポスト2015開発アジェンダの実現を可能にする要素であることを確認する。

1.3 また、情報通信技術（ICT）の普及により支援される、社会全体における情報と知識へのアクセス拡大が、持続可能な開発を支援し人々の生活を向上させることを確認する。

テクノロジー（ICT）の普及により支援される情報と知識へのアクセス拡大が、持続可能な開発を支え、人々の生活を向上させることを確認する。

1.4 インターネット関連の法律、ポリシー、プロトコルを国際人権法と整合させることを促進する。

1.5 人権に基づく、すべての人にアクセス可能なオープンなインターネットを促進し、マルチステークホルダー参加を特徴とするインターネット普遍性原則（R.O.A.M）を支援する。

1.6 ユネスコの全プログラム活動において、インターネットの横断的役割を強化する。これには「優先課題：アフリカ」「優先課題：ジェンダー（ジェンダー平等）」、小島嶼開発途上国及び後発開発途上国への支援、並びにユネスコが主導する「文化の相互理解のための国際10年」が含まれる。

2. 情報・知識へのアクセス分野におけるユネスコの選択肢：

2.1 情報と知識への普遍的、開放的、手頃な価格での制約のないアクセスを促進し、デジタル格差（ジェンダー格差を含む）を縮小する。オープンスタンダードを奨励し、意識向上を図り、進捗を監視する。

2.2 若年層、障害者、周縁化・脆弱な立場にあるこの集団を含む市民参加を保証する、開放性、透明性、説明責任、多言語主義、包摂性、ジェンダー平等を基盤とする政府原則に導かれた、アクセス向上を図るICTポリシーを提唱する。

2.3 国連総会で合意された持続可能な開発目標（SDGs）の策定、実施、進捗監視への市民参加を促進する革新的な手法を支援する。

2.4 公共アクセス施設の創設を奨励し、あらゆるタイプのユーザーが情報・知識の創出者・利用者としてインターネットを活用する能力を育成することを支援することにより、情報・知識及びICTへの普遍的アクセスを促進する。

2.5 学術・科学・ジャーナリスト情報のオープンアクセス、政府データの公開、フリー・ソフトウェアが、オープンな知識資源の構築に重要な貢献をしていることを再確認する。

2.6 インターネットが文化的多様性にもたらす可能性を探求する。

3. 表現の自由分野におけるユネスコの選択肢

3.1 加盟国及びその他の関係主体に対し、インターネット上における表現の自由及び情報・思想の自由な流通に関する国際人権法の保護、促進及び実施を強く求める。

3.2 表現の自由は、オンライン上でもオフライン上でも適用され、尊重されるべきであることを再確認する。これは、世界人権宣言第19条及び市民的及び政治的権利に関する国際規約（ICCPR）第19条に基づき、情報への自由に対するいかなる制限も
市民的及び政治的権利に関する国際規約第19条第3項に規定される国際人権法に準拠しなければならないことを再確認する。

3.3 ジャーナリスト、メディア労働者、ソーシャルメディア制作者（特にジャーナリズムを大量に生み出す者）の安全を支援し、
インターネット上・オフラインを問わず、表現の自由やジャーナリズムに対する攻撃が刑事免責に終わらないよう、法の支配による刑事免責との闘いの重要性を再確認する。

3.4 インターネット及びデジタル通信に関連する国際条約として、障害者権利条約（CRPD）、女性に対するあらゆる形態の差別撤廃条約（CEDAW）、及び差別、敵意、暴力への扇動を構成する民族的、人種的、宗教的憎悪の助長禁止に関する人権高等弁務官事務所の活動（2012年ラバト行動計画）の関連性を認識し、
表現の自由を制限する手段としてこれを利用することなく、オンライン上の憎悪表現と闘うための教育・社会的仕組みを促進する。

3.5 インターネット仲介業者が表現の自由の促進と保護において果たす重要な役割に関する対話を継続する。

4. プライバシーに関するユネスコの選択肢

4.1 デジタル監視、データ収集・保管・利用、その他の新たな動向がプライバシーに与える影響を評価する研究を支援すること。

4.2 世界人権宣言第12条及び市民的及び政治的権利に関する国際規約第17条に基づき、プライバシー権がオンライン・オフラインを問わず適用され尊重されるべきであることを再確認する。またユネスコの権限の範囲内で、デジタル時代におけるプライバシー権に関する国連総会決議A/RES/69/166に関連する取り組みを支援する。

4.3 加盟国及びその他の関係者が、国際人権義務に従ってインターネット上の安全保障及びプライバシー上の懸念に対処するための最良の慣行及び取り組みを支援し、この点において民間セクターの関係者が果たす重要な役割を考慮する。

4.4 匿名性と暗号化がプライバシー保護と表現の自由の促進手段として果たし得る役割を認識し、これらの問題に関する対話を促進する。

4.5 個人情報の収集において、正当性・必要性・比例性を確保し、データ内の個人識別情報を最小化する手法に関するベストプラクティスを共有する。

4.6 オンライン上のプライバシー権に関する人々の認識向上、政府や商業企業が情報を収集・利用・保存・共有する手法の進化、デジタルセキュリティツールによるユーザープライバシー権保護手法の理解促進を図る取り組みを支援する。

4.7 ユーザーに安全、権利尊重、救済手段を提供し、新たなデジタルサービスへの信頼を強化する個人データ保護の取り組みを支援する。

5. 情報社会の倫理的側面に関するユネスコの選択肢

5.1 新たなテクノロジーや新興テクノロジーがもたらす影響と社会的インパクトについて、人権に基づく倫理的考察、研究、公的対話を促進する。

5.2 生涯学習プログラムを含む教育コンテンツ・資源の中核要素として、人権に基づく倫理的考察の理解と実践、ならびにオンライン・オフライン双方の生活におけるその役割を支援する内容を取り入れること。

5.3 女の子と女性が、オンライン・オフライン双方の障壁を取り除く積極的措置を講じ、平等な参加を促進することで、ジェンダー平等に向けたインターネットの可能性を最大限に活用できるようにする。

5.4 政策立案者が包括的な知識社会における人権に基づく倫理的側面に対処する能力を強化できるよう、関連する研修と資源を提供すること。

5.5 インターネットの越境的性質を認識し、地球市民教育、地域・国際協力、能力構築、研究、ベストプラクティスの交換を促進し、その倫理的課題に対応するための幅広い理解と能力の開発を図る。

6. 横断的課題に関するユネスコの選択肢：

6.1 メディア・情報リテラシー（MIL）に関するユネスコの専門知識を、公式・非公式教育システムに統合することを促進する。これは、デジタルリテラシーとインターネット上での情報への普遍的アクセス促進が、人権理事会決議26/13で列挙された教育権の促進において重要な役割を果たすことを認識したものである。

6.2 デジタル時代におけるジャーナリズムの情報源の機密性保護強化の必要性を認識する。

6.3 加盟国に対し、要請に基づき、関連する国内法・ポリシー・慣行を国際人権法と調和させることを支援する。

6.4 情報社会における全ての主体がポリシー及び慣行の策定・実施において透明性と市民参加を促進することを支援する。

6.5 研究の促進：法律、ポリシー、規制枠組み、インターネットの利用に関する研究を推進する。これには、研究の主要分野における関連指標の活用を含む。

6.6 情報・知識へのアクセス及び表現の自由の分野に関連するネットワーク中立性に関する議論へのユネスコの参加を促進する。

7. ユネスコの役割に関する選択肢

7.1 国連システム内におけるユネスコの貢献とリーダーシップを強化する。これには、WSIS成果の継続的実施、WSIS+10レビュー、IGF、ポスト2015開発アジェンダが含まれる。

7.2 国連システム外のパートナー（各国政府、市民社会、報道機関、学術界、民間セクター、技術コミュニティ、個人ユーザーなど）と適切に関与する。これには専門的助言の提供、経験の共有、対話の場づくり、ユーザーの能力開発とエンパワーメントの促進が含まれる。

7.3 加盟国が、インターネットポリシーと規制において全ての利害関係者の参加を確保し、国際的な人権とジェンダー平等を統合するよう支援する。

付録2：インターネットの普遍性に関するユネスコ概念論文

インターネットの普遍性：知識社会とポスト2015持続可能な開発アジェンダ構築への手段

2013年9月2日

要約

ユネスコのコミュニケーション・情報部門は、「インターネットの普遍性」という新たなコンセプトを提唱している。これは、知識社会への進展とポスト2015年持続可能な開発アジェンダの策定に向けた継続的な条件を包括的に強調する役割を果たしうる。このコンセプトは、インターネット、モバイル、ICTへの普遍的アクセスを含むが、それを超えるものである。「普遍性」という言葉は、これまでのインターネットの広範な進化に体現されてきた四つの基本的規範を指し、複数の異なる側面がより広範な全体の一部であるという包括的な理解の枠組みを提供する。インターネットがその歴史的潜在能力を十分に発揮するためには、以下の強さと相互依存性に基づく完全な「普遍性」を達成する必要がある：(i) インターネットが人権に基づく規範（本論文では「自由なインターネット」の実質的意味）、(ii)「開放性」の規範(iii)「全ての人にアクセス可能」であることを強調する規範、(iv) マルチステークホルダー参加によって育まれる規範である。これら四つの規範は、R – O – A – M（権利、開放性、アクセシビリティ、マルチステークホルダー）という語呂合わせで要約できる。「インターネット普遍性」のこのコンセプトは、特にユネスコにとって極めて具体的な価値を持つ。ユネスコの既存のインターネットに関する立場を基盤とすることで、このコンセプトは、2014年から2021年までの戦略期間におけるユネスコの教育、文化、自然科学・社会科学、コミュニケーション・情報分野におけるインターネット関連活動の多くを枠組み化するのに役立つ。インターネットガバナンスに関する国際的な議論において、『インターネットの普遍性』というこのコンセプトは、ユネスコが国際的なマルチステークホルダー協力を促進する上で役立つ。また、ポスト2015年持続可能な開発アジェンダにユネスコが貢献できる点を強調するのにも役立つ。

作成：表現の自由・メディア開発部 コミュニケーション・情報部門[241]

* 本文の完全版は国連公用語でオンライン公開中：

http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/ unesco-internet-study/internet-universality/

241 ユネスコ部門間協議及び外部協議からの知見を反映。また、このコンセプトの策定への貢献に対しコンスタンス・ボンメラー氏に謝意を表する。

要約版（4ページ）

1. なぜ「インターネットの普遍性」というこのコンセプトが必要なのか？

ユネスコは、インターネットが世界をより平和に、持続可能な開発と貧困撲滅に近づける膨大な可能性を秘めていることを長年認識してきた。[242] グローバルな使命のもとで活動し、普遍的な価値観を推進する国際政府間組織として、ユネスコはインターネットの「普遍性」と論理的な関連性を持つ。この「普遍性」は、インターネットに関連する四つの主要な社会的側面、すなわちこのインフラが普遍的な規範に基づいている度合いを貫く共通の糸として理解できる。具体的には：(i) 人権に基づく（したがって自由な）
(ii) 開放性；(iii) すべての人へのアクセス可能性；(iv) 多様な利害関係者の参加。これら四つの規範は、R-O-A-M（権利、開放性、アクセス可能性、多様な利害関係者）という頭字語で要約できる。

様々なステークホルダーは、表現の自由、オープンなアーキテクチャ、セキュリティ問題、オンライン倫理など、それぞれが本質的と捉える特徴に基づいてインターネットを特徴付けてきた。[243]この多様な概念化が示すのは、懸念や利害の多様性であると同時に、インターネットそのものの多面的な性質である。これを受けて、様々な考慮事項や次元が互いに、またより広範な全体とどのように関連しているかを理解する可能性について疑問が生じる。この大きな全体像を概念化する方法として、ユネスコは現在「インターネットの普遍性」という概念を検討している。これはマクロ概念として機能しうる。その目的は、広大で複雑かつ進化し続けるインターネットの永続的な本質を捉え、様々な関係者、特にユネスコがインターネットとどのように関わるかを包括的に理解することを容易にすることにある。このコンセプトは、インターネットが社会においてますます中心的な役割を果たす中、特に教育、科学、文化、コミュニケーション・情報分野における「インターネット化」の進展という文脈において、有効な視点として特に役立つ可能性がある。

「インターネット普遍性」のこのコンセプトは、ユネスコにとって特に重要な四つの規範を特定するとともに、これらを相互に補強し依存し合う特性を認識できる形で、単一の統合的な枠組みにまとめている。このような包括的な知的デバイスがない限り、ユネスコのインターネット関連活動間の相互関連性や、それが知識社会やポスト2015持続可能な開発アジェンダにどう貢献するかを把握するのは困難だろう。

ユネスコの国際的議論への関与に関して、『インターネットの普遍性』このコンセプトは、統合的・包括的枠組みとしての可能性を有すると考えられる。一方で「インターネットの自由」といった既存概念と共通する自由と人権の原則を強調し、他方でアクセスと利用の絡み合った課題、ならびに

242 例えば：「ユネスコによるインターネットに関する考察と分析：ユネスコと専門分野におけるインターネットの活用」（2011年）。http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/ED/ICT/pdf/useinternetdomains.pdf。

243 例えば、ストックホルム・フォーラム、サイバースペースに関するオンライン自由連合、ウィルトン・パーク、ロンドンおよびブダペストのサイバースペース大会では、それぞれ異なる重点が置かれてきた。同様に、インターネットは国際機関によって多様な形で分析されてきた。具体例としては、欧州評議会議の「インターネットの普遍性、完全性及び開放性の保護と促進に関する閣僚委員会の勧告CM/Rec(2011)8」（2011年）、OECD理事会「インターネット政策策定の原則に関する勧告」（2011年）、OSCEメディア自由担当代表「インターネット2013大会からの勧告」（2013年）、ICC「インターネット上の表現の自由と情報の自由な流通に関するポリシー声明」、インターネット権利原則連合「インターネット権利原則憲章」（2010年）。

技術的・経済的開放性の問題も含まれる。さらに、このコンセプトはマルチステークホルダーの関与を不可欠な要素として包含している。このように包括的な形で、「インターネットの普遍性」というこのコンセプトは、南北間の対話や異なるステークホルダー間の対話を橋渡しする先見的な枠組みとなり得る。したがって、グローバルなインターネットガバナンスの議論やポスト2015持続可能な開発アジェンダの形成に独自の貢献をもたらす可能性もある。

2. 「インターネット普遍性」概念の解明

インターネットの「普遍性」を構成する四つの規範的要素の結びつきは、ユネスコの従来のインターネットに関する考え方に密接に基づいている。これには以下が含まれる：

- *多言語主義の促進及びサイバースペースへの普遍的アクセスに関する勧告*（2003年）。[244]（この文書は特にアクセシビリティ規範と権利の均衡の必要性を指摘している）。
- *ユネスコによるインターネットに関する考察と分析*（2011年）。[245]（この文書は、ユネスコのプログラムに関連する規範的作業と、マルチステークホルダー参加を強調している）
- *WSIS+10レビューイベント最終勧告*及び*WSIS+10レビューイベント最終声明*（2013年）。[246]（権利、アクセス、開放性、マルチステークホルダー問題などを網羅している）。
- *UNGIS（国連情報社会グループ）によるポスト2015持続可能な開発アジェンダに関する共同声明*（2013年）。[247]（この文書は、包括的な知識社会に貢献するための情報テクノロジー全般、特にインターネットにとっての社会的条件の重要性を強調している）

「インターネットの普遍性」は、既存のユネスコの知見を統合し、インターネットとユネスコが既に認識している知識社会の基盤となる基本原則（表現の自由、すべての人への質の高い教育、情報と知識への普遍的アクセス、文化的・言語的多様性の尊重）[との]関連性を示す。このコンセプトは、インターネットが知識社会実現の手段となるために必要な要素を浮き彫りにする。これは、インターネットの特性と有用性が技術的・社会的・法的・経済的その他の仕組みを伴い、それらがこのインフラの積極的可能性を支える特定の規範に依存していることを示すための方法論的枠組みとして機能する。より深く考察すると、「インターネットの普遍性」を構成するR-O-A-M規範（権利、開放性、アクセシビリティ、マルチステークホルダー）は以下のように理解できる：

(i) インターネットと人権に基づく規範との関連性を自由の構成要素として特定することで、「インターネットの普遍性」は以下のような調和の持続を強調するのに役立つ：

---

244 http://www.unesco.org/new/en/communication-and-information/about-us/how-we-work/strategy-and-programme/promotion-and-use-of-multilingualism-and-universal-access-to-cyberspace/.

245 http://unesdoc.unesco.org/images/0019/001920/192096e.pdf;

246 第1回WSIS+10レビューイベント「平和と持続可能な開発のための知識社会に向けて」の文書、2013年2月25日～27日、パリ：http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_recommendations_en.pdf;http://www.unesco.org/new/fileadmin/ MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_final_statement_en.pdf

247 http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/ungis_joint_statement_ wsis_2013.pdf.

248 *ユネスコによるインターネットに関する考察と分析*、http://unesdoc.unesco.org/.

images/0019/001920/192096e.pdf。

インターネットの成長と利用、そして人権。この意味での自由なインターネットとは、人権の行使を尊重し、可能にするものである。[249]この点において、「インターネットの普遍性」は、表現の自由、プライバシー、文化的参加、ジェンダー平等、結社の自由、安全、教育など、様々な人権とインターネットの間の相互依存関係や相互関係を幅広く考慮するよう私たちに求める。

(ii) 「インターネットの普遍性」はまた、インターネットが「オープン」であるべき規範を強調する。この指定は、オープンスタンダードといったテクノロジー的課題の重要性、ならびに知識と情報へのオープンアクセス基準の重要性を認めるものである。オープン性はまた、アクターの参入の容易さと、独占によって課される可能性のある閉鎖性の不在の重要性をSignalする。

(iii) 「インターネットの普遍性」の規範としての「すべての人へのアクセス可能性」は、技術的アクセスや利用可能性の問題、経済的所得や都市・農村格差に基づくデジタルデバイドなどを提起する。したがって、最低限の接続インフラへの普遍的アクセスに関する規範の重要性を示唆している。同時に、「アクセシビリティ」は、識字能力、言語、階級、ジェンダー、障害などの要因に基づくインターネットからの社会的排除に対処することを要件とする。さらに、人々がいわゆる情報・サービスだけでなく、コンテンツ・コード・アプリケーションの生産者としてインターネットにアクセスすることを理解すれば、ユーザーの能力の問題は「普遍性」のアクセシビリティ次元の一部である。これはユネスコのメディア・情報リテラシー概念を浮き彫りにする。同概念は、インターネット利用者が批判的・有能的・倫理的に関与する力を強化することでアクセシビリティを高める。

(iv) この意味でインターネットは「供給側」からの視点だけでは捉えられず、補完的な「ユーザー中心」の視点が必要だ。「インターネットの普遍性」における参加型、特にマルチステークホルダーの関与という側面は、様々なレベルでインターネットの開発と政府において、異なる主体（様々な分野や社会的・経済的地位を代表する主体、女性と女子も除外しない）が果たしてきた役割、そして今後も果たすべき役割の理解を促進する。参加は、このインフラが平和、持続可能な開発、貧困撲滅にもたらし得る価値にとって不可欠である。対立するステークホルダーの利害を調整する上で、参加型メカニズムはインターネットの悪用を緩和する共通規範の形成に寄与する。ここでの「普遍性」はインターネットの共有政府を強調するものである。

これら四つの側面における規範はそれぞれ異なるが、相互に補強し合う。権利がなければアクセシビリティは少数者に限定され、アクセシビリティがなければ権利はアクセス可能性の潜在力を阻害する。開放性は共有と革新を可能にし、権利尊重とアクセシビリティを補完する。マルチステークホルダー参加は他の三つの規範を保証するのに役立つ。全体として、人権尊重、開放性、アクセシビリティ、マルチステークホルダー参加のいずれかを欠くインターネットは、定義上、普遍性から程遠いものとなる。

3. 「インターネットの普遍性」というこのコンセプトがユネスコに関連する方法

ユネスコは「インターネットの普遍性」を推進する上で独自の役割を担っている。ユネスコは社会生活全般をカバーする権限を持つ国連機関であり、その枠組み内で以下に関わるプログラムを実施している。

249 このように、「インターネットの普遍性」は、国連特別報告者による「意見及び表現の自由の権利の促進及び保護に関する報告書」と一致し、また2012年に国連人権理事会が採択した「インターネット上における人権の促進、保護及び享受」に関する最初の決議にも呼応するものである。

教育、文化、科学、社会科学、コミュニケーション・情報分野におけるインターネット活用を包含する。ユネスコは「インターネットの普遍性」を包括概念として用いることで、モバイル学習、女の子教育、文化的・言語的多様性、メディア・情報リテラシー、気候変動研究、表現の自由、情報への普遍的アクセス、生命倫理、社会的包摂など、より具体的な課題の位置付けが可能となる。このように「インターネットの普遍性」は、ジェンダー平等やアフリカ支援といった優先課題の推進にも寄与し得る。この概念は、ユネスコ全体のインターネット関連業務を包括的かつ統合的に支える枠組みとして機能し、全事業に共通の参照枠を確立する。運用面では、このコンセプトにより様々な取り組みが「インターネットの普遍性」を共同で推進するイニシアチブとして位置付けられる。相乗効果や部門間協力、共同プログラム策定を促進し得る。特に、2014-2021年中期戦略（37/C4）及び4カ年プログラム（37/C5）への理解を深める効果がある。

4. 結論

「インターネットの普遍性」は、以下の点で本機関が広範な国際社会に提供するサービスと合致する：

- アイデアの実験場（先見性を含む）— このコンセプトの構築は、ユネスコの創造的・シンクタンクとしての潜在能力に直接関連する。
- 世界的な議論を喚起することで、「インターネットの普遍性」は、ユネスコが包括的かつ包摂的なアプローチで国際協力の触媒となり得ることを示す。
- 規範設定者としての役割 – このコンセプトが広く支持されれば、「インターネットの普遍性」の進捗を監視する基準策定の指針となり得る。
- ポリシー立案の指針となり、官民・市民社会・意思決定者を巻き込む規範的枠組みとして、「インターネットの普遍性」はユネスコが加盟国における能力構築機関としての役割を果たす助けとなる。

将来的に、「インターネットの普遍性」は、ユネスコがこれまで提唱してきた「無形文化遺産」や「知識社会」といった影響力のある知的成果の足跡を辿る可能性がある。このコンセプトは時代の新たな概念化を体現しているため、複雑でダイナミックな人類の創造物に関する世界的な議論に貴重な貢献をもたらし、インターネットが人類の共有する未来に継続的に貢献することを促進する役割を果たすだろう。

ユネスコ・インターネット自由シリーズ

ユネスコは2009年より、インターネットの自由に関する旗艦シリーズ刊行を開始した。これはインターネットの法・ポリシー課題の変遷を探求し、加盟国やその他の関係者にネット上の表現の自由を促進する環境づくりに向けたポリシー提言を提供することを目的としている。

本シリーズの第8弾となる本書の過去刊行物は以下の通りである：

プライバシー、表現の自由、透明性：
デジタル時代における新たな境界の再定義

本研究は、インターネット環境における表現の自由の権利、プライバシーの権利、透明性の価値の相互作用を分析する。権利の均衡を図る法的枠組みと現行のメカニズムを網羅し、具体的な問題、事例、動向を提示する。国家機関、インターネットユーザー、ICT企業、市民社会組織、司法、治安機関といった複数のプレイヤー間の相互作用を想定し、関係者に提言を行う。

インターネット政府の原則

ユネスコインターネット自由シリーズの第6弾となる本研究は、50以上の宣言、ガイドライン、枠組みについて定量的・定性的評価を行っている。これらの文書に含まれる課題は、アクセス、表現の自由、プライバシー、倫理、優先課題であるジェンダー平等、優先課題であるアフリカ、持続可能な開発など、ユネスコの関心分野の文脈で評価されている。

オンライン上のヘイトスピーチ対策

本研究は、オンラインのヘイトスピーチを特徴づける動態と、それを阻止・緩和するために採択するために採用された対策のいくつかについて、地域レベルおよびグローバルレベルで生まれた優れた実践例を強調しながら、世界的な概観を提供する。本出版物は、国際的、地域的、国家的な規範的枠組みの包括的な分析を提供し、特に、オンラインの憎悪メッセージの生成、拡散、影響に対抗するのに役立つ社会的・非規制的メカニズムに重点を置いている。

ジャーナリズムのためのデジタル安全構築：選定課題の調査

テクノロジーが発展するにつれ、ジャーナリズムに対する機会と脅威も拡大している。本研究はデジタル時代におけるジャーナリズムの安全に対する新たな脅威を説明し、ジャーナリストのためのデジタル安全構築を支援する枠組みを提案する。ジャーナリスト通信のハッキングからメディアウェブサイトへのサービス拒否攻撃まで、ジャーナリズムに対する12の主要なデジタル脅威を検証し、それらを回避するための予防的、保護的、先制的な対策を評価している。また、ジャーナリズムのデジタルセキュリティは技術的側面を含むが、それを超えるものであることも示している。

オンライン上の自由を育む：インターネット仲介業者の役割

インターネット上でコンテンツ作成者と視聴者の仲介役を果たすインターネット仲介業者の台頭を受け、このユネスコ出版物は、インターネット仲介業者が表現の自由やプライバシーなどの関連する基本的権利に与える影響について、詳細な事例研究と分析を提供する。また、仲介業者と国家がインターネット利用者の表現の自由の権利の尊重を改善する方法に関する政策提言も提示している。

インターネット上のプライバシーと表現の自由に関する世界調査

本出版物は、表現の自由とインターネットプライバシーの関係性を明らかにし、様々な状況下で両者が互いに補完し合うか競合するかを評価する。表現の自由の観点から、現在のインターネットプライバシー規制環境における課題を整理する。法的保護、自主規制ガイドライン、規範的課題、関連事例研究の概要を提供する。

接続の自由、表現の自由：インターネットを形作る変化する法的・規制的生態系

本報告書は、表現への脅威の背景にある社会的・政治的力学について新たな視点を提供する。この問題の議論において考慮すべきポリシーと実践の広範な文脈を論じるため、「表現の自由の生態系」に関する概念的枠組みを構築する。

全出版物は以下からダウンロード可能だ：

http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/unesco-internet-study/

人権と暗号化

本出版物は、2015年11月の第38回大会で承認されたユネスコのインターネット問題に対する新たなアプローチに沿ったものである。加盟195カ国は「CONNECTing the Dots成果文書」を採択するために採用する。この文書にはユネスコの今後の行動指針として38の選択肢が示されている。また「インターネット普遍性原則（R.O.A.M.）」も採択され、人権に基づく開放的でアクセス可能なインターネットを提唱し、マルチステークホルダー参加によるガバナンスを主張している。

暗号化は、現在のインターネットガバナンスに関する国際的な議論におけるホットトピックである。本研究はこの主題を掘り下げ、様々な暗号化手段、その利用可能性、メディア・通信環境における潜在的なアプリケーションについて、世界的な概観を示す。研究では、暗号化の導入が法や政策の異なる領域によってどのように影響を受けるかを説明し、選定された法域における暗号化の詳細な事例研究を提供する。

メディア・通信環境における暗号化の役割と、各種サービス・組織・エンドユーザーへの影響を詳細に分析する。この調査・分析に基づき、多様なステークホルダーに有用な暗号化ポリシーに関する提言を行う。これには、現行議論におけるジェンダー感度の欠如への対応必要性の指摘や、「暗号化リテラシー」向上のためのアイデア提示も含まれる。

コミュニケーション・情報部門

国際連合教育科学文化機関

UNESCO

9 789231 001857