話し合いの再**構築**：暗号化の議論を深く掘り下げる

*政府は、暗号化は法執行機関の**業務の遂行**を妨げると述べていますが、この技術は子**ども**やその他**弱い立場に置かれている**人々を含むすべての人を保護**するものです。***

2024年2月

作成者：
ヘザー・ウェスト|シニアディレクター
+1 202.344.4597
HEWest@Venable.com

ザック・マーティン|シニアポリシーアドバイザー
+1 202.344.4393
ZPMartin@Venable.com

アイビー・オレッキオ |プロジェクトマネージャー
+1 202.344.4277
IDOrecchio@Venable.com


CENTER FOR
CYBERSECURITY
POLICY AND LAW

目次

エグゼクティブ・サマリー

暗号化は、オンライン通信の保護、言論の自由の実現、金融取引の保護など、データのプライバシーとセキュリティにおいて重要な役割を果たします。 Center for Cybersecurity Policy & Lawは、サイバーセキュリティコミュニティの多くのステークホルダと同様に、暗号化を弱めることは、すべての組織と個人のセキュリティ、プライバシー、自由権、および重要な社会的利益を危険にさらすと考えています。

暗号化は、個人情報の盗難や違法な監視などの犯罪から個人を保護しますが、法執行機関や国家安全保障機関は、暗号化により、法執行機関が犯罪や公共の安全に対する脅威を調査することがより困難になる、または不可能になると主張しています。デジタル時代の捜査においては、公共の安全、テロ、児童性的虐待のコンテンツ（CSAM）に関連する傍受および復号化された通信を含む、デジタルエビデンスが必ず要求されるとの主張もあります。

暗号化の反対派は、私たちが実際には、対立する者に対して共通の利害によって団結しているにも関わらず、これを2つの対立する立場の者による論争として捉えています。 暗号化は、子どもやその他の弱い立場にある人を含むすべての人を保護します。
ソーシャルメディアサイトやメッセージングアプリケーションを含むテクノロジー企業は、自社のプラットフォームが犯罪活動や違法なコンテンツの経路になることを望んでいません。

この論文の著者は、話し合いを再考する時が来たと考えています。 したがって、政府と法執行機関は、暗号化を回避できるユビキタスな監視を義務付けるのではなく、法執行機関とオンラインセキュリティに影響を与える政策と法律に対して実用的で漸進的なアプローチを取る必要があります。

この文書では、下記の内容に言及します。

- 暗号化ポリシーに関する歴史的な議論と論拠を検討する。
- 現在の政策や法律の文脈において提案されている内容から繰り返されるテーマをレビューする。
- 最新の暗号化の議論をどのように進めるべきかを確立する。そして
- 話し合いが変わらない場合の、潜在的な課題に取り組む。

Center for Cybersecurity Policy & Lawについて

Center for Cybersecurity Policy & Lawは、政府、民間産業、市民社会にセキュリティ脅威をより適切に管理するための実践とポリシーを提供することにより、世界中のサイバーセキュリティを強化することを目的とする独立した組織です。
Venable LLP（脆弱な顧客ケアポリシー）のサイバーセキュリティサービスグループ内の501 (c)(6)非営利団体として2017年に設立された当センターは、政策の専門知識をグローバル、国家、および地域レベルにおける招集力と組み合わせて、業界のリーダーと政策立案者を結びつけ、実際の成果を生み出すための連携とイニシアチブの立ち上げを行っています。 センターでは、コンセンサス指向のリスク管理ベースのアプローチを適用し、デジタルインフラストラクチャと情報システムのセキュリティ保護において最前線にいる人々の視点と実践から引き出された実用的なソリューションと政策提言を促進することにより、サイバーセキュリティをめぐる複雑さを解明し、混乱を解消することを目指しています。

はじめに

テクノロジーは私たちの日常生活に根付いています。 インターネットはまさに文字通り私たちの手の届くところにあり、ダイヤル式電話はFaceTime通話やZoomミーティングに取って代わり、手紙はショートメッセージや電子メールへと変わり、ウェアラブルデバイスは私たちの健康に関するリアルタイムの実態として、心拍数、血糖値、その他の健康指標のデータの追跡を提供します。 通信技術とモノのインターネットによって、私たちの現実は拡張し、世界のどこにいても、友人、家族、コミュニティとのつながりを維持しています。 これらのデジタル技術の活用が拡大する中、企業は安全性を確保するために努力してきており、多くの場合、暗号化を使用してデータを保護しています。

私たちのデジタル環境におけるこれらの顕著な進歩に加えて、犯罪者や悪意のある行為者もこれらの技術を使用しています。法執行機関や国家安全保障機関など、社会を守る責任を負う組織は何十年もの間、これらの技術におけるセキュリティと暗号化メカニズムが彼らの本来の任務を妨げていることを懸念し、その責任はテクノロジー企業にあると非難の矛先を向けています。

そのように反応するのは簡単かもしれません。プライバシーとセキュリティは我々のテクノロジーに組み込まれており、ますます当たり前になっています。 暗号化は、重要な個人データを保護するための実装として中核を担うものです。 法執行機関の提案は単純です。暗号化された内容へのアクセスを許可し、有害な内容を特定するためにメッセージをスキャンするシステムをセットアップすることを提案しています。当局者は、彼らの提案が子どもたちを保護し、違法薬物を街から排除し、汚職を防止し、暴力犯罪を阻止するのに役立つ可能性を述べています。しかし、これらの過度に単純化されたソリューションは非常に危険であり、プライバシーを侵害し、個人を悪意のある行為者や盗聴者にさらす可能性があります。 それにもかかわらず、プラットフォームがエンドツーエンドのメッセージングの暗号化とデバイス上のデータの暗号化に移行するにつれて、法執行機関と政策立案者は例外を求め続けていますが、これらの提案は、すべての人のデジタルライフを安全に保つために暗号化が果たす重要な役割を十分に説明していません。

暗号化は、情報を安全に保つために不可欠です。 企業は過去50年間、データを侵害から保護するだけでなく、通信と運用を保護するために暗号化を使用しており、多くのセクター（ヘルスケア、金融サービス、教育を含む）では、法律やベストプラクティス、標準などいずれによってかにかかわらず、データを暗号化することが業界において要求されています。 法執行機関、軍、および政府関係者も、暗号化の重要性に同意しており、同じツールと技術を使用して自分達のシステムとデータを保護しています。 しかし、これらの公共機関の多くは、子どもと公共の安全を保護するという名目で暗号化を回避する方法を望んでいます。 残念ながら、1人のために暗号化を破ることは、保護しようとしている人々を含め、ほぼ確実にすべての人のために暗号化を破ることになります。

「暗号化をめぐる論争」または「暗号戦争」を相反する勢力の衝突として特徴づけることは、その核心にある共通の目標と相互の利益を損なうことになります。 この論争の中の重要な問題、特に児童の性的虐待とCSAMとの戦い、そしてテロ対策の取り組みは、技術の進歩とは無関係に存続しています。 犯罪活動は新しい出来事ではなく、インターネットや暗号化以前から存在しています。ソーシャルメディアプラットフォームとメッセージングアプリケーションを運営するテクノロジー企業は、自社のプラットフォーム上にこれらの内容が掲載されることを望んでおらず、それを防ぐために多大な資金を費やしています。[1] 表面に現れない部分で、子どもと一般市民を保護するために、そもそも最初からこれらの犯罪が発生するのを防ぐという共通の大義が、これらの一見対立する集団を一つに結びつけています。

[1] https://www.thorn.org/blog/new-report-shows-an-increased-effort-by-tech-companies-to-detect-csam-on-the-internet/

このような共通の取り組みにもかかわらず、共通のソリューションに向けた大きな進展は依然として見られないままです。社会からこれらの問題を根絶することができる普遍的な解決策や、特効薬、魔法の杖のようなものはなく、場合によっては提案された解決策が非常に危険な諸刃の剣になる可能性を認識することが不可欠です。

たとえば、最近の活動としては、オンラインクラウドストレージプラットフォームのiCloudで、CSAMを検出するためのAppleの取り組みが特に取り挙げられています。 広告掲示板には、人工知能が生成した顔が隠された子どもの画像が以下の文章とともに掲載されました。「児童の性的虐待がiCloudに保存されている。Appleはそれを許可している。」これは、エンドツーエンドで暗号化されているかどうかにかかわらず、iCloudに保存されている画像をスキャンしてCSAMを探すためのプライバシーとセキュリティを保護するシステムの開発を中止するというAppleの決定に反応したものですが、それは問題の真相ではありません。[2] 長年の研究の後、Appleは「すべてのユーザーの個人的に保存されたiCloudデータをスキャンすると、データを盗み取ろうとするものが見つけ、悪用するための新しい脅威ベクトルが作成される」と判断しました。 また、意図しない結果として非常に危険な道筋が作られる可能性があります。 たとえば、1つのタイプのコンテンツをスキャンすると、一括監視を行う扉を開くこととなり、コンテンツの種類を超えて、他の暗号化されたメッセージングシステムを検索したいという欲求が生じる可能性があります。」[3]

したがって、暗号化をめぐる論争は複雑さと課題を抱えながら続いており、あらゆる集団がシンプルな解決策を模索しています。 誤解しないでいただきたいのは、Center for Cybersecurity Policy & Lawは、子どもや一般市民の安全が最優先であるものの、他のすべての公的および民間部門の組織および個人のプライバシーとセキュリティを危険にさらすことなく犯罪と戦うための効果的な方法は存在すると考えます。 そうはいうものの、私たちはその完璧さを求め進歩を敵に回すことはできません。可能な解決策について議論しながら、プライバシーとセキュリティを強化し、コミュニティを守ることができる段階的なステップを見失ってはなりません。 暗号化を回避するという方策は、技術的および政策的な課題に満ちており、安全に利用を広めることは不可能ではないにしても困難です。 私たちは、デジタルエコシステム全体とそれを使用するすべての人を保護するセキュリティを損なうことなく、公衆と子どもの安全を保護する方法があると確信しています。

暗号化に関する歴史的な議論

ロバート・レッドフォードとシドニー・ポワチエが主演した1992年の映画「*スニーカー*」では、暗号化技術者があらゆる暗号化スキームを解読し、視界から隠れたものを復号化できるデバイスを作りました。 政府のハッキング事件に続き、法律に違反した後に新しいアイデンティティを名乗っていたロバート・レッドフォードと彼のチームは、デバイスにつながる仕事のために雇われ、その後倫理的なジレンマに直面することになります。 世界中のどのシステムからでも情報にアクセスする権限をすぐ手に入れることができましたが、それはやりすぎではないでしょうか？ 最終的にレッドフォードのチームはその通りであると判断し、彼はデバイスを破壊し、それを望む悪意のある者と法執行官の両方を阻止しました。

この映画は30年以上にわたって観客を楽しませてきましたが、暗号手法は外交、スパイ活動、戦争の遂行に使用されているため、その核心にある難題は何世紀にもわたって議論されてきました 。 歴史を通じて、シークレットコードと暗号の使用は、安全な通信を維持し、機密情報を保存するために不可欠でした。 この論争は勝ち負けを繰り返しながら、犯罪は阻止されてきました。 しかし、それらが使用されているということは、潜在的な脅威や敵対者が違法行為のために同じツールや技

[2] CSAM（児童性的虐待）写真検査ツールを止めるAppleの決断が新の論争を巻き起こす ”
https://www.wired.com/story/apple-csam-scanning-heat- initiative-letter/
[3] Ibid

術を利用するのを防ぐ必要性が高いということです

現代のデジタル暗号化に対する議論は、公共のインターネットより前から存在し、冷戦時代に重要な役割を果たしました。 第二次世界大戦後、米国は通信のための暗号化技術を中心に輸出管理を実施し、強力な暗号化技術の輸出を禁止しました。 米国のように、多くのヨーロッパ諸国は当初、強力な暗号化技術は軍事用途を有する可能性のある弾薬またはデュアルユース品目であると見なして、強力な暗号化技術に厳格な輸出規制を課していました。[4] これはいく分の成功を収めましたが、一般的には米国を含む世界中で弱い暗号化の使用につながりました。[5]

1990年代には、暗号化の議論が進化しました。 商用インターネットの立ち上げと特に金融取引におけるパーソナルコンピュータの普及により、暗号化はより主流になりました。 FBIと国家安全保障局（NSA）は、通信におけるエンドツーエンドの暗号化の使用に公然と反対し始めました。[6] 1993年、彼らは政府がクリッパーチップと呼ばれる暗号化された通信へのアクセスを取得できるようにするデバイスを提案しました。[7]このチップは、サードパーティー（この場合は政府）が復号化キーにアクセスして、暗号化されたコンテンツを読み取ることを可能にする概念であるキーエスクローを使用しようとするものです。 最終的には、粗末で安全性の低い設計により人権擁護活動家とプライバシー擁護派からの怒りとが相まり勝利を収めたため、今日の携帯電話には、法執行機関が会話を聞くことができるチップが搭載されてはいません。

1996年、39カ国がデュアルユース技術を含む輸出管理に関するワッセナー協定に署名しました。安全性の低い形式の暗号化は、この協定の下で輸出管理されなくなりました。[8]米国内では、セキュリティと暗号化による自由（SAFE）法によって、冷戦時代の政策によって生じた問題に対処しようと検討がなされました。 何十年もの間、強力な暗号化製品は厳しく規制されており、海外での販売を禁止したり、より弱い「輸出グレード」バージョンの輸出が必要とされていました。 超党派による法制化では、国家安全保障と技術の進歩、個人の権利の間でバランスをとる必要性が強調されました。ソフトウェア企業は、既存の輸出規制がイノベーションを抑制していると主張し、数十年前の政策には効果がなく、米国経済に悪影響を及ぼしていることを示す証拠を示しました。[9] SAFE法は成立しませんでしたが、1999年秋、クリントン政権は、小売暗号化製品の輸出制限の撤廃を含む、法案の条項のほぼすべてを実施する方針を採択しました。[10]

これらのグローバルなポリシーの変更に対応して、NSAは強力な暗号化の基礎となる暗号化標準を弱めるために密かに取り組み始め、公衆の監視がないバックドアを作成しました。[11] 2006年までに、NSAは仮想プライベートネットワークをクラッキングすることによって3つの航空会社、旅行予約システム、外国政府の原子力部門、その他別の政府のインターネットサービスへのアクセスを取得しました。

---

[4] Ihttps://carnegieendowment.org/2019/05/30/encryption-debate-in-european-union-pub-79220、https://www.sciencedirect.com/science/article/abs/pii/B9780444516084500274?via %3Dihub

[5] 「玄関マットの下の鍵: 全てのデータと通信への政府のアクセスを要求して危険な状態を命じること」http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence = 8

[6] 「暗号化の現状：議論がどのように変化したか」、https://opensource.com/article/18/6/listening - susan - landau

[7] “クリッパーチップの短命と恥ずべき死” https://gizmodo.com/life - and - death - of - clipper - chip - encryption - backdoors - att - 1850177832

[8] https://www.armscontrol.org/factsheets/wassenaar

[9] https://slate.com/technology/2015/06/safe-act-the-right-to-strong-encryption-almost-became-law-in-the-90s.html

[10] https://www.govinfo.gov/content/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2399.pdf

[11] https://www.brookings.edu/articles/a-brief-history-of-u-s-encryption-policy/

これは、2013年のスノーデンの暴露によって明らかになり、暗号化キーを生成するために使用される乱数ジェネレータに侵入することによって、どのようにスパイ機関が暗号化された通信にアクセスしたかが文書化されていました。[12]

マサチューセッツ工科大学（MIT）の2015年の技術報告書は、2000年代初頭に暗号化されたコンテンツへのアクセスを可能にすることには問題があり、そしてインターネットが進化し、重要性が高まっていることによって、現在はさらに悪化する可能性があることを明確にしています。[13]「何百万ものアプリとグローバルに接続されたサービスを備えた今日のインターネット環境の複雑さは、新しい法執行機関の要件が、予期しない検出困難なセキュリティ上の欠陥をもたらす可能性があることを意味する」と報告書は述べています。 「これらやその他の技術的脆弱性を超えて、グローバルに展開される例外的なアクセスシステムの見通しは、そのような環境がどのように統治されるか、そのようなシステムが人権と法の支配を尊重することをどのように保証するかについて、困難な問題を提起しています。」

NSAは情報にアクセスする手段としてネットワークの脆弱性を活用するよう方針を変えましたが、FBIは暗号化との次の戦いの最前線にとどまりました。 2015年、英国と米国の政治・法執行機関の指導者たちは暗号化が犯罪を捜査する法執行機関の能力を脅かすとして、再び暗号化に反対の立場を述べました。[14]

カリフォルニア州サンバーナーディーノでの大量銃乱射事件の後、再び最前線の議論として浮上しました。 FBIは、さらなる手がかりを追跡するために、銃撃者のiPhoneのPINを解読すること（デバイスの復号化）をAppleに要求するよう裁判所に対し求めましたが、テクノロジー企業は拒否しました。[15]最終的に、FBIはデバイスに侵入することができるサードパーティの企業を見つけましたが、これによって政府によるメッセージやデバイスへの裏の侵入経路に係る考えが再び明らかになりました。 当時、法律が提案されましたが、どれも前進しませんでした。 これは、Appleにデバイスの復号化を強制しようとする最も注目を集めたケースでしたが、これが唯一のケースではありませんでした。Appleは少なくとも5回の試みを認めましたが、いずれの試みも支持されませんでした。[16][17] FBIが実際にデバイスにアクセスした際には、新しい情報は見つかりませんでした。[18]

[12] https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted = 2 &_ r = 2
[13] “Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications,” http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence = 8
[14] Ibid
[15] サンバーナーディーノとApple対FBIの1年後、我々は今暗号化のどこにいるんですか？」 https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption
[16] https://www.justsecurity.org/wp-content/uploads/2016/03/Apple-All-Writs-Apple-Requests-Received-Letter.pdf
[17] https://www.theguardian.com/technology/2016/feb/23/apple-new-iphone-models-san-bernardino-shooter-all-writs-act-department-of-justice
[18] https://www.theverge.com/2016/4/19/11463672/apple-fbi-san-bernardino-iphone-contents-no-leads

繰り返されるテーマ及び現在の政策と法律

暗号化の議論を通して、**強力な暗号化の使用を違法とする**いくつかの提案が暗号化アルゴリズムと暗号化されたコンテンツへのバックドア**やフロントドア**を**めぐって**浮上し**ました。**

提案	課題
仲介アクセス（キーエスクロー） ：信頼できるサードパーティが暗号化キーを保持し、特定の条件が満たされたときに暗号化されたデータへ法執行機関**が**アクセス**できるようにする方法**	サードパーティのセキュリティと信頼性は、不必要なリスク（誤用、不正アクセスなど）をもたらす可能性があります。 キーの所有者が標的になると、壊滅的な攻撃を引き起こす可能性があります。 キーを再構築または転送する必要がある場合、データへの**迅速**なアクセスは困難です。
仲介されていないアクセス： データ所有者または**処理者**からの関与なしに暗号化データにアクセスするための法執行機関によるツールと技術の**導入**。	法執行機関が使用するバックドアは、悪意のある行為者によって悪用されたり、権限のないユーザーに悪用されたりする可能性もあります。 データ主体の知識または同意なしにデータにアクセスすることは、さまざまなプライバシー、公民権、または**自由権**の問題を**生じさせる**可能性があります。
技術支援： ハイテク企業が、暗号化を弱めたり、データを復号化するツールを作成したりすることで、法執行機関が暗号化されたデータにアクセスする手助けをするよう強制されるプロセス。	ツールやバックドアを作成すると、システムが弱体化し、攻撃に対してより脆弱になります。 ハイテク企業は、自社の製品が法執行機関のために意図的に弱体化されていると**考えるのであれば**、ユーザーの信頼を失う可能性があります。 テクノロジー企業は、コンプライアンス要件を見越して、デフォルトで弱いシステムを構築するかもしれません。

過去数年間の提案により、法執行機関と政府がこれらの暗号化攻撃を構成する方法が変わりましたが、潜在的な影響は変わっていません。

英国のオンライン安全法

2023年9月、英国は、ウェブサイトやその他のインターネットベースのサービス**が**違法で有害なコンテンツ**を含まないようにする**ことを目的とした**オンライン安全法**[19]**を可決しました。** この法律は、検索エンジン、ソーシャルメディアプラットフォーム、ユーザー生成コンテンツのホスト、オンラインフォーラム、ゲーム、ポルノサイトなど、幅広いオンラインサービスプロバイダに適用されます。[20]

同法はエンドツーエンドの暗号化を明示的に禁止していませんが、政府が承認した技術を使用したコンテンツのフィルタリングと年齢確認が**義務付けられることに**なります。 提案には、エンドツーエンドの暗号化メッセージングを提供するハイテク企業にCSAMのメッセージコンテンツ**の**スキャンを義務づけ当局に報告できるようにする条項も含まれていました。[21] これはハイテク企業からの強い反対を受けましたが、承認された法律に含まれる追加の改正案では、企業は「技術的に実現可能であり、**児童の性的虐待および搾取的なコンテンツのみを検出するための最低限の正確性基準を満たしていると技術が認定されるまで」**暗号化されたメッセージをスキャンする必要はないと述べられています。[22]

[19] https://bills.parliament.uk/bills/3137
[20] 「議論の余地のある英国のオンライン安全法案が法律になるようである。」 https://www.computerworld.com/article/3706810/uks-controversial-online-safety-bill- set-to-become-law.html
[21] https://www.gov.uk/government/publications/end-to-end-encryption-and-child-safety/end-to-end-encryption-and-child-safety
[22] https://subscriber.politicopro.com/article/2023/09/u-k-dials-up-fight-with-meta-over-encryption-00117008?source=email

しかし、暗号化ポリシーの歴史は、この面で何が技術的に実現可能であるかについて、法執行機関、テクノロジー企業、および技術者の間に広く意見が分かれていることを示しています。

人気メッセージングアプリ、Signalは、暗号化バックドアを要求される場合、英国市場での運用を停止すると述べています。[23] 英国内務省はまた、FacebookとInstagramのエンドツーエンドの暗号化を展開するMetaに反対するキャンペーンを開始しました。グラフィック言語を使用して、検出されない可能性があるCSAMを説明しています。 あるビデオでは、児童性的虐待の被害者がMetaチーフのマーク・ザッカーバーグに直接申し立てを行い、暗号化の展開計画を再考するよう訴えています。[24] オンライン安全法が可決された後、英国内務省の圧力にもかかわらず、[25] Metaは長期的な計画のもと、メッセンジャーのエンドツーエンドの暗号化を開始して、[26] 年末までに暗号化されたWhatsApp製品に 参加し、プラットフォーム上のすべてのメッセージを覗き見る必要のない方法を使用して、グルーミングと児童虐待コンテンツを共有するためプラットフォームに対する監視を継続するとしています。[27]

オーストラリアの支援およびアクセス法

法律を通じて暗号化の使用を抑制しようとしているのは英国だけではありません。 オーストラリアは、デジタル時代に効果的に運用し、テロと犯罪に対処するために必要なツールを法執行機関と情報機関に提供するために、2018年に支援及びアクセス法を可決しました[28] が、暗号化に対する攻撃であるとして広く説明されてきています。[29]

この法律は、機器の製造、ソフトウェアの開発または更新、またはウェブサイトの運営に関与する通信サービスプロバイダ、企業、または個人に対し、法執行機関や治安当局と協力する責任を増やしました。 また、法執行機関向けのコンピューターアクセス令状を作成し、捜索令状を介してアカウントベースのデータにアクセスし、コンピューターやモバイルデバイス上の暗号化されていないデータに対する治安当局の捜索と差し押さえの権限を強化しました。[30]

この法律の重要なメカニズムには、データへの特別なアクセスのための任意および強制的な要求、ならびに組織が独自の暗号化の解読、ダウングレード、またはバックドアの構築を含む新しい機能の構築を含む支援を提供することを組織に要求する条項が含まれます。[31]

---

[23] https://twitter.com/mer_edith/status/1704477739871273397

[24] https://subscriber.politicopro.com/article/2023/09/u-k-dials-up-fight-with-meta-over-encryption-00117008?source=email

[25] https://www.reuters.com/technology/uk-urges-meta-not-roll-out-end-to-end-encryption-messenger-instagram-2023-09-19/

[26] https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/

[27] https://www.theguardian.com/technology/2023/jun/07/meta-instagram-self-generated-child-sexual-abuse-materials

[28] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

[29] https://www.eff.org/deeplinks/2018/12/new-fight-online-privacy-and-security-australia-falls-what-happens-next

[30] https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/

[31] https://www.abc.net.au/news/2018-12-04/encryption-whatsapp-signal-messages-explained/10580208

この法律は、その可決のスピード、透明性の欠如、および不十分な協議プロセスに関して、ハイテク企業、プライバシー擁護者、および一般市民から継続的な批判を受けています。 法律に組み込まれた**セーフガード措置**は、業界に暗号化を破るように要求すること**はできないとされています**が、批評家は、企業にアクセスのための新しい機能を作成することを強制する**この**法律の力が、企業に**よる**暗号化を弱体化させたり、バックドアを構築したりすることを強制するために使用される可能性があると主張しています。 オーストラリア人の情報セキュリティを損なうことで、この法律は広範囲に影響を及ぼし、世界中の企業や人々の情報を危険にさらす可能性があります。

2020年6月現在、強制**的な**命令は**公表**されておらず、**作成された支援要請は**20件未満**となっています**。[32]

その他の提案

世界中の各国政府が暗号化に**対し**さまざまなアプローチを取っています。 以下は、要約と潜在的な影響を含む、世界中で提案され、可決された政策と法律の表です。

国名	法律	概要	暗号化への影響
インド	2000年情報技術法第69A条（可決）	この法律の下で、インド政府は、インターネットサービスプロバイダ（ISP）や通信サービスプロバイダを含むオンライン仲介業者に、国家安全保障への脅威とみなされるコンテンツや情報をブロックするよう指示する権限を**有し**ます。[33]	今年初め、インド政府はこの法令を利用して、テロリストに通信を可能にし、国全体のアクセスをブロックしているとされる14の暗号化されたメッセージングアプリを禁止しました。
欧州連合	児童の性的虐待を防止し、これに対抗するための規制（提案**された**児童の性的虐待規制、CSAR ）	この提案では、当初、プロバイダーがサービス上のCSAMを検出、報告、削除することが要求されました。 これらの規則により、サービスプロバイダーは、暗号化されたメッセージを含むCSAMおよびチャイルドグルーミングのためにサービスを積極的にスキャンする必要があります。[34] 欧州議会の市民の自由、司法、および内務委員会（LIBE）は、この条項を削除し、的を絞った監視のみを許可することを採択しました。[35]	欧州議会が実施した影響評価では、最初の提案はエンドツーエンドの暗号化とデジタル通信のセキュリティを損ない、すべての通信メタデータのスクリーニングは相応でない、または必要ではないという欧州司法裁判所の先例に違反する可能性が高いと結論付けられました。[36] 議会は後に検出命令の要旨を逸脱しない範囲でエンドツーエンドの暗号化を含む案を採択し、他の緩和策が有効でない場合にのみ使用する必要があることを明確にしました。最終案では、ターゲットを絞った監視のみが許可されています。[37]

[32] https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/30904 d 8 b -7 cfb -4 ef 0 -99 fb - fba 2299 b 57 bf /& sid = 0000

[33] https://tutanota.com/blog/posts/apps-banned-india

[34] https://cyberlaw.stanford.edu/blog/2023/06/eu-member-states-still-cannot-agree-about-end-end-encryption

[35] https://edri.org/our-work/csar-european-parliament-rejects-mass-scanning-of-private-messages/

[36] 欧州議会。 （2023年4月）。 補完的影響評価ー児童の性的虐待を防止し、撲滅するための規則を定める規制の提案。 https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU (2023) 740248_EN.pdf

[37] https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass-surveillance

英国	調査権限法（IPA）による規制改正	IPAは、特別なアクセスに関する広範な要件を設けており、この更新には、グローバル市場に影響を与える可能性のある新しいセキュリティ技術を事前承認またはブロックする機能が含まれています。[38]	現行のIPAでは、暗号化の弱体化、制限、またはバックドアを含むすべてのユーザーのサービスを英国政府が変更することを許可しているようです。 また、企業は、エンドツーエンドの暗号化などセキュリティ機能の導入を含む、調査に影響を与えるような方法にサービスを変更する前に、政府に通知する必要があります。[39]
アメリカ	虐待および横行するネグレクトを排除するためのインタラクティブ技術法（EARN IT法）	この法律は、オンラインでの児童の性的搾取防止に関する全国委員会を設立し、通信品位法の第230項を改正してサービスプロバイダーの保護を取り除き、既存のCSAM法の施行を強化することにより、児童の搾取に対処することを目的としています。[40]	EARN IT法は、サービスプロバイダーがエンドツーエンドの暗号化を削除するか、バックドアを作成することを奨励し、子どもやその他の影響を受けやすいグループを含むすべてのユーザーに脆弱性をもたらします。 さらに、委員会によって開発されるベストプラクティスは政治的に推進される可能性があり、指名されたメンバーの大部分は議会の指導者らによって任命されます。

最新の暗号化議論を解き明かす

カーネギー国際平和基金（Carnegie Endowment for International Peace）、プリンストン大学（Princeton University）、国際技術政策センター（Center for International Technology Policy）は、 *新しい*アプローチを見つけることを目標に、暗号化の議論を慎重に検討するために暗号化ワーキンググループを結成しました。 彼らは、2019年に「Moving the Encryption Policy Conversation Forward（暗号化ポリシーの会話を前進させる）」を発表しました。[41] グループは、暗号化されたデータへの法執行機関のアクセスをめぐる行き詰まりに対処するための提案されたアプローチの利点とリスクの両方を含め、暗号化の社会的影響を評価するためのより有益な方法を提案しています。 この論文では、特に携帯電話の暗号化に焦点を当て、法執行機関へのアクセスに焦点を当てた提案を評価するためのより具体的なアプローチを詳述しています。

カーネギーの論文は、このトピックを公平かつ複数の利害関係者からの視点で捉え、暗号化への賛成と反対の2つの主要な議論を否定することから始めています。これらは次のとおりです。

1. 法執行機関は、暗号化された情報へのアクセスを可能にするアプローチの模索をやめるべきです。
2. 法執行機関は、合法的なプロセスを通じてすべての暗号化されたデータへのアクセスを取得できない限り、公衆を保護することはできません。

最終的に、グループは、追加の作業が必要であり、携帯電話の暗号化ユースケースには進展する可能性があると結論付けました。 重要なポイントは次のとおりです。

- 携帯電話で保存されている暗号化データを議論することは、関心のある多様なコミュニティ間の議論を可能にし、リスクと利益のより明確な評価が行いやすくなります。

[38] https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-overview#what-does-the-investigatory-powers-amendment-bill-do

[39] https://www.justsecurity.org/87615/changes-to-uk-surveillance-regime-may-violate-international-law/

[40] https://tutanota.com/blog/posts/earn-it-barr-encryption

41 https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573

- この分野における既存の提案が実行可能であること、将来の提案が実行可能であること、または現時点でポリシーの変更が推奨されることなどを示す兆候はありません。
- このトピックについてすべての立場を踏まえて誠意を持って議論することができなければ、この包括的な暗号化の議論はできなさそうです。

重要な最初のステップは、共通点を確認することです。 この議論には、私たち全員が合意できると考えている要素があります。

暗号化は、ほとんどの組織でデータを保護し、人々が本人であることを証明するための最良の防御策です。 また、社会保障番号、支払いカード情報、その他の個人情報を侵害するなど、重大なデータ侵害が発生しており、今後も引き続き発生しますが、暗号化は情報を保護するための最善の手段です。[42] 逆に、犯罪者がキーストアがあること、または暗号化アルゴリズムにロック解除ができる入り口があることを知っている場合、それは犯罪者にとって非常に魅力的なハニーポットであるという証明になり、犯罪者は自分の目的のためにそのロック解除しようと最善を尽くします。

漸進*的な変化が前進するための鍵* となります。 これまでの議論は、過度に単純化された解決策によって特徴づけられてきました。 現代の暗号化の議論では、テクノロジーの急速な進歩により、これらのシステム内で複雑さと相互運用性へ対処しようとすることがどのように標的として動いてしまうものであるかを認識する必要があります。 「広範で例外的なアクセスを実現するためには、新しいテクノロジー機能が展開され、文字通り世界中の何十万人もの開発者と共にテストがなされる必要があります」とMITの報告書は述べています。 「これは、類似の技術を使用する傾向にあり、新機能から生じうる脆弱性を管理するためのリソースを備えている可能性が高い、電気通信やインターネットアクセスサービスにおいて、現在活用されている電子監視よりもはるかに複雑な環境です。」 暗号化を使用し、コンテンツの送信や保存に役立つ製品やサービスの数が増えているため、例外的なアクセスの問題の複雑さが増しています。

ことわざにあるように、敵の敵は味方でもあります。 ソーシャルメディアサイトやメッセージングアプリケーションを含むテクノロジー企業は、自社のプラットフォームが犯罪活動や違法なコンテンツの経路になることを望んでいません。これらのプラットフォームおよびサービスの運営者は、事業を行う管轄区域で、CSAMおよびその他の違法コンテンツの拡散を防止するために取り組んでいます。
コンプライアンスだけが、このコンテンツを検出して削除するために取り組む唯一の理由ではありません。組織は、他のユーザー、社会、およびビジネスへの信頼を保護しています。

政府と法執行機関は、意図しない結果を避けるために、暗号化に影響を与える政策と法律に対して実用的で計画的なアプローチを取る必要があります。 政府や法執行機関にあらゆる種類のバックドアを有効にすると、インターネットがより複雑になり、さらなる脆弱性につながり、すべてがさらに安全ではなくなります。[43] これらのバックドアにアクセスするための資格情報が破損した場合、壊滅的な事態となり、攻撃者は法執行機関がアクセスできるのと同じ情報にアクセスして復号することができます。

この論文の著者は、こうした議論を再考する時が来たと考えています。 暗号化の議論は2つの対立する陣営で構成されていますが、実際には私達は同じ敵と戦っています。 段階的な進歩に向けて焦点を移すことが不可欠です。 この論文の残りの部分では、議論が変わらない場合の潜在的な課題について取り上げます。

---

[42]https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

[43] https://defense360.csis.org/bad-idea-encryption-backdoors/

政府のガバナンス

技術者は、セキュリティに大きな影響を及ぼすことなく、暗号化されたコンテンツへのアクセスを可能にすることはほぼ不可能である、というのが技術者の間で一致している認識です。しかし、技術的な課題は、そのような例外的なアクセスシステムのガバナンスにおける課題と対になっているでしょう。[44] 数え切れないほどの法律、多くの管轄区域、多数の利害関係者がアイデアを出し、それぞれが貴重な、しかししばしば矛盾する視点をもたらしています。 暗号化されたコンテンツへの例外的なアクセスのための包括的なガバナンス構造を確立するには、誰が議論に参加すべきか、暗号化されたデータにアクセスするための正当な目的は何か、利害関係者が要求に応じたりコンテンツを積極的に共有したりするための現実的な時間枠など、意見の相違を調整することが必要です。

こうした問題のうちの1つを1つの国の中で解決することでさえ、困難な作業です。 例えば、米国内の多数の法執行機関や機関職員が安全にセキュリティを維持しながら通信にアクセスし、復号化できるようにすることは非常に困難です。 おそらく、調整メカニズムとして機能するFBI管轄の一元化されたクリアリングハウスを構築し、連邦、州、地方の法執行機関がそれを利用できるようにするための司法メカニズムを構築することが考えられます。 例外的なアクセスシステムのサポート要員を多数雇用したり、暗号化をダウングレードしたり、例外的なアクセスシステム自体のセキュリティを維持しようとする企業に迅速に対応するためのシステムを設計するかもしれません。企業や監督機関は、特にデータ需要が対外的に口外することを禁止されている場合、いつ、誰によって、どのような状況で顧客データにアクセスされるかを正確に追跡する際に重大な課題に直面するでしょう。

この複雑さは国際的な規模ではさらに悪化します。なぜなら、それぞれの要求を誰が管理できるかという問題は、それほど単純には答えが得られないためです。そのため、いくつかの企業は、暗号化回避策が法律になった場合、特定の国での事業を止めると述べています。[45]

さらに、ガバナンスは、資格情報とツールがどのように管理されるかという点に対処する必要があります。 当局がするべきではないことのためにシステムを使用しないように、厳格なポリシーと手続きを制定する必要があります。[46]多くの大手テクノロジー企業やその他の情報源からのユーザー情報を監視しているNSAの様々な監視プログラムを使用すれば、低レベルのアナリストでさえ、監視されることなく情報にアクセスすることができました。 この機関にはLOVEINTという名前さえついており、従業員がこれらのツールを使用して、恋愛対象者、配偶者、監視対象外の人々を監視していました。[47] 最近、米国の裁判所は、FBIが犯罪の疑いのある米国人を含め、数年間にわたり米国の外国情報機関のデータベースで278,000回、不適切に情報を検索したことを明らかにしました。[48]

また、NSAのギガバイト相当の武器化されたソフトウェアエクスプロイトをリークした個人またはグループであるシャドーブローカーによって証明されているように、政府は自らのセキュリティ侵害から免れることはできません。[49] この侵害には、ほとんどのバージョンのMicrosoft Windowsを標的とするエクスプロイトとハッキングツール、および世界中のいくつかの銀行のSWIFT銀行システムに対する巧妙なハッキングの証拠が含まれていました。 そして、米国人事管理局の2, 150万件の職員記録の侵害、

[44] https://www.accessnow.org/secure-the-internet/

[45] https://www.theverge.com/23409716/signal-encryption-messaging-sms-meredith-whittaker-imessage-whatsapp-china

[46] https://www.newyorker.com/news/amy-davidson/america-through-the-n-s-a-s-prism

[47] https://slate.com/technology/2013/09/loveint-how-nsa-spies-snooped-on-girlfriends-lovers-and-first-dates.html

[48] https://www.reuters.com/world/us/fbi-misused-intelligence-database-278000-searches-court-says-2023-05-19/

[49] https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

米国国立公文書記録管理局による7,600万人の軍人の記録、インドのアーダール識別番号、スウェーデン運輸庁、米国有権者データベースのデータ侵害など、他の多くの事例があります。[50]

暗号化バックドアは、弱い立場にある人々を攻撃するために使用される可能がある

ガバナンスと密接に関係するのは、暗号化バックドアが権威ある立場の人々によって政治的反対派、宗教団体、その他の少数派を抑圧するために悪用される可能性があるという懸念です。暗号化は、権威主義国の反体制派や迫害を受けている人々など、弱い立場にある人々の言論の自由を保護する上で重要な役割を果たしています。 多くのテクノロジー企業は、これまで人権への影響がある要求には従わないことを選択してきました。 たとえば、ユーザーのセクシュアリティ、政治活動、または所属に関するデータを転用すると、重大な罰則が科せられる可能性があります。 米国では、議員らは、犯罪に関連する場合は法執行機関にアクセスを許可する必要があると主張するでしょうが、ほかの国では、このアクセスは人権侵害につながる可能性があります。

バックドアに関する命令については、ハイテク企業にはいくつかの選択肢があります。ハイテク企業は、すべての政府に対して同じ対応をすることができますが、これは人権侵害に加担することになる可能性があります。 あるいは、個々の要求をケースバイケースで評価することもできます。この場合、完全な情報がないまま評価することになりますが、人権侵害の可能性もなくなります。[51]

暗号化に反対する歴史的な議論は、特に脆弱な人々に対する犯罪との戦いに重点を置いています。 しかし、これらの議論はまた、政治的反対者を沈黙させるために国際的に使用されてきました。[52] 今年初め、インドの技術法の下、14のメッセージングアプリケーションが、テロリストによって使用されていたという名目で国内で禁止されました。[53] この禁止は、インド政府からの公聴会や通知もなく行われ、プラットフォーム運営者を驚かせました。

国連の代表者は、抑圧的な政権の標的になる可能性のある個人を保護するために暗号化を重要なものとして支持するという意見を表明しました。 「暗号化ツールは、人権擁護者、市民社会、ジャーナリスト、内部告発者、迫害やハラスメントに直面している政治的反体制派などによって世界中で広く使用されています」と、国連人権高等弁務官ザイド・ラアド・アル・フセイン（Zeid Ra 'ad Al Hussein）は2016年に述べています。[54] 「表現および意見の自由と、プライバシーの権利の両方を実現するためには、暗号化と匿名性が必要です。 暗号化ツールがなければ、生命が危険にさらされる可能性があると言っても過言ではありません。 最悪の場合、政府が市民の電話に侵入する能力があることは、純粋に基本的人権を行使しているだけの個人の迫害につながる可能性があります。」

暗号化により、標的にされる可能性のある人は自由にコミュニケーションをとることができます。 「一般のインターネットユーザー、人権擁護者、野党政治家、政治活動家、調査を行っているジャーナリストは、外部の干渉から通信を保護することによってのみ

---

[50] https://www.executech.com/insights/the-5-scariest-data-breaches-in-government/

[51] https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

[52] https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

[53] https://internetfreedom.in/14-mobile-apps-banned/

[54] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID = 17138#sthash.o25R7Bqg.dpuf

サイバー犯罪や世界中の政府の詮索の目から自分自身を守ることができます」と、2016年のアムネスティ・インターナショナルの報告書は述べています。[55]

法執行機関の代理としてのハイテク企業

近年、議論は、暗号化バックドアを必要とする法執行機関から、有害な内容が送信されていないことを確認するためにメッセージをスキャンする必要があるハイテク企業へと移りつつあります。 企業がこのようなメッセージを見つけたとき、適切な当局に通知するかは企業次第です。 これは最近、法案が提案され可決された法律の中核であり、ハイテク企業を事実上の法執行機関の役割に据えるものです。

2021年、オーストラリアはオンライン安全法を通じて既存の保護を拡大および強化しました。この法律は、基本オンライン安全見込み（Basic Online Safety Expectations）を[56]オンラインサービスプロバイダに導入し、違法および制限されたコンテンツに対する強制的な業界規範を求めています。[57] さらに最近では、カリフォルニア州知事ギャビン・ニューサムが10月に、「故意に児童の商業的性的搾取を促進、幇助、または教唆する」役割を果たしたサービスを罰する法案に署名しました。[58] 欧州連合はまた、メッセージングプラットフォームがCSAMをスキャンすることを望んでいますが、これらのプラットフォームによるユビキタスな監視を促進することの懸念に基づいて、検出命令の範囲からエンドツーエンドの暗号化を除外しています。[59]

法律や政策は、テクノロジー企業に対し、CSAMやその他の違法行為が疑われる場所の特定にさらに積極的に取り組むよう奨励することで、セキュリティとプライバシーを確保し守りながら情報にアクセスする必要がある法執行機関のニーズとのバランスを見つけようとしています。 その結果、ハイテク企業は、自社のデジタル製品や自社が保持するユーザーデータを保護するよう求めながら、それと同時に法執行機関や情報機関がより多くのデータにアクセスできるようにしようとしている、議員や政策立案者との間で板挟みになっています。

「議員たちは、暗号化の重要な役目を半減させるという賢明ではない使命に着手しました」と、タラ・ウィーラー氏とジェフリー▸カイン氏は外交問題評議会のブログに書いています。[60]「彼らは、警察がバックドアを介してデジタルホームに入ることを許可する一方で、ほかのすべての人には暗号化の鉄の正面ゲートを維持するという法的例外を要求しています。」 しかし、他の人がバックドアを探さないだろうと信じるのは現実的ではありません。

こうした「中道」とされる道を行くことで、ハイテク企業は潜在的に有害なコンテンツを特定しながら、エンドツーエンドの暗号化を維持することができるでしょう。しかし、専門家は、これらのクライアント側のスキャン技術は「ユーザーのプライバシーと暗号化によるセキュリティの保証を

---

[55] https://www.amnesty.nl/content/uploads/2016/03/160322_encryption_-_a_matter_of_human_rights_-_def.pdf

[56]https://www.esafety.gov.au/industry/basic-online-safety-expectations

[57] https://www.esafety.gov.au/newsroom/whats-on/online-safety-act

[58] https://www.firstpost.com/tech/news-analysis/californias-governor-signs-ban-penalising-social-media-platforms-for-aiding-or-abetting-child-abuse-13229372.html

[59] https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass-

surveillance

[60] https://www.cfr.org/blog/theres-cop-my-pocket-policymakers-need-stop-advocating-surveillance-default

中身のないものにする」と考えています。[61] エンドツーエンドの暗号化サービスでCSAMを見つけるためのワーキングプロトタイプを構築した人でさえ、これらの技術は危険であると考えています。[62] これらのスキャンシステムは、監視や検閲のために簡単に再利用でき、世界中のテクノロジー企業への要求は、政治的反体制派、宗教的少数派などを標的にしたいという願望があることを証明しています。

政府は、そもそもハイテク企業を法執行機関の代理として務めるような状況に置くべきではありません。[63] 企業に法執行機関の立場に立つよう求めることは、重要な境界線を曖昧にし、従業員をユーザー、企業、政府への義務の間で、本質的に利益相反が生じる立場に置くことになります。 そして、企業が代理を務め、このような調査を行うよう要請され、危害や権利侵害に加担してしまった場合、誰が責任を問われるのかは明らかではありません。

暗号化を無効にすることだけが犯罪者を捕まえる唯一の方法ではない

暗号化を破るよう繰り返し求められているにもかかわらず、暗号化されたデバイスやメッセージに侵入することが、犯罪者を捕まえる最善の方法であるかどうかは明らかではありません。 2018年、戦略国際問題研究所（CSIS）は「Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge（簡単に実現できる成果：デジタルエビデンスの課題に対するエビデンスに基づく解決策）」を出版しました。[64] この報告書は、犯罪捜査を妨げる暗号化についての政府と法執行機関の懸念は一部のケースで正当なものであるものの、単一で簡単な解決策は存在しないと述べています。 実際、連邦、州、および地方自治体の法執行機関関係者からの調査回答によると、関連するデータ（その多くは暗号化されていない）を持つサービスプロバイダーを特定できないことが、それらのケースでデジタルエビデンスを使用する能力に関する最大の問題であることが示されました。 この報告書では、法執行機関向けのデジタルエビデンストレーニングにおけるギャップに目を向けています。 これには、証拠の収集や証拠保全を担当する職員のほか、請求手続きに不可欠な裁判官も含まれます。[65]

この知識とスキルのギャップは現実世界に影響を及ぼし、さまざまなテクノロジーがどのように機能し、デジタルエビデンスがケースを裏付けるためにどのように使用されるかについて、非現実的な期待をもたらす可能性があります。 2017年、FBIは、情報を収集するために7,000台の暗号化されたデバイスに侵入することはできないと言及しましたが[66]、実際は1,000から2,000台であることが判明しました[67]。FBIの捜査総監からの報告書によると、FBIは、サンバーナーディーノ事件でAppleにハッキングを強制するよう裁判所に依頼する前に、電話へのアクセスを徹底的に試みていなかったことが判明しました[68]。しかし、多くの場合、デバイスは捜査官が望むほど役に立ちません。 知識や経験に富んだ犯罪者は、自らの計画を明らかにする可能性が低く、私たちと同じようにメッセージを使う、つまり明確な文脈のない短いメッセージを大量に使用することが多い傾向にあります。多くの場合、それらのデバイスには法執行機関が捜査に取り掛かるために役立つであろう情報が存在すらしていない可能性があり、[69]報告書には代替の証拠やその他の手段を使用して解決された事件の件数は示されていませんでした。

[61] https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption

[62] https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/

[63] https://www.cfr.org/blog/theres-cop-my-pocket-policymakers-need-stop-advocating-surveillance-default

[64] https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf

[65] Ibid

[66]https://www.bbc.com/news/technology-41721354

[67] https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html

[68] https://www.washingtonpost.com/world/national-security/inspector-general-fbi-didnt-fully-explore-whether-it-could-hack-a-terrorists-iphone-before-asking-court-to-order-apple-to-unlock-it/2018/03/27/b56a9dca-31cf-11e8-8abc-22a366b72f2d_story.html

サンバーナーディーノ事件をめぐるすべての論争の後、FBIはデバイスから有用な情報を探り出したことはありません。[70]

犯罪者を捕まえるためにデジタル時代にもたらされた伝統的な捜査手法には、依然として役割があります。 たとえば、ロシアのスパイ、アンナ・チャップマンは彼女の情報を暗号化し、パスワードを書き留めましたが、それが当局によって発見され、情報にアクセスするために使用されました。 違法なシルクロード市場のリーダーとされる人物を捕まえるために、捜査官はその人物がコンピュータにログインするまで、デバイスを取り上げずに待ちました。[71] FBIの全令状法のケースでは、電話はハッキングによって解読され、友人や家族にパスコードを共有するよう依頼することさえありました。

多くの場合、具体的なメッセージの内容は必要ではない場合があります。 米国では、法執行機関や情報機関は、従来の法的手続きを通じて捜査に役立てるために、メタデータやトラフィック分析などの他のデータを取得することができます。[72] この点で米国は有利です。企業は本社の所在地ではなく、その施設の所在地に基づいて要件を課されることが増えているものの、最大の通信サービスプロバイダの多くが米国にあり、米国の法律の対象となるため、外国の法執行機関は、米国の法執行機関よりもはるかに悪い状況にあります。しかし、民主的な政府にサービスを提供する情報機関の間にも強力なパートナーシップがあり、協力によって複雑な世界的事件を終結させることもしばしばあります。[73]

ただし、これらの手法を使用するには、法執行機関がどこで通信情報を探せば良いかを知る必要があります。 トレーニングセンターやデジタルエビデンス収集に関するさまざまな取り組みに適切な資金を提供することで、国の法執行機関や情報機関だけでなく、あらゆるレベルの法執行機関は、他の課題につながる可能性のある暗号化バックドアに頼ることなく、これらの事件を調査するための準備を整えられるでしょう。[74]

米国では、州および地方の法執行官および法律専門家にデジタルエビデンストレーニングを提供する国立コンピュータ科学捜査研究所（National Computer Forensics Institute：NCFI）に対して、適切に資金を提供することが1つのステップとなるでしょう。 2018年、政府はNCFIの完全撤廃を提案しました。 議会がそれに気づいて資金が回復したのち、ようやくNCFIは救済されましたが、後年、科学捜査トレーニングへの資金は80 %以上削減されました。[75] 同様に、欧州連合法執行協力庁（Europol）は、EU全体の犯罪情報と国家協力の調整ハブとして機能し、トレーニングとデジタル科学捜査のためのリソースを一元化する理想的な場所となるでしょう。科学捜査トレーニングは、社会のあらゆるレベルで法執行に役立つ可能性がありますが、CSAMやその他の公的な脅威と戦うための現代の犯罪捜査のために、この基本的で中核的なトレーニングが含まれている提案はほとんどありません。

---

[69] https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

[70] https://www.theverge.com/2016/4/19/11463672/apple-fbi-san-bernardino-iphone-contents-no-leads

[71] Ibid

[72] https://www.justsecurity.org/79549/we-now-know-what-information-the-fbi-can-obtain-from-encrypted-messaging-apps/

[73]https://www.lawfaremedia.org/article/rethinking-encryption

[74] https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf

[75] Ibid

同様の組織やトレーニングプログラムは、犯罪行為の捜査に苦慮しているすべての国の公共の安全に役立つでしょう。

デジタルエビデンスを入手するとすぐに、法執行機関はその証拠の管理に苦心することになります。 戦略国際問題研究所（Center for Strategic and International Studies）の最近の 報告書 では、法執行機関の職員を調査し、職員の多くが実際には、コンピュータ対応型犯罪だけでなく、一般的な犯罪を調査するために必要なデータをどのようにテクノロジー企業に対して基本的な要求として行うのか知らないことが明らかになりました。[76]

これらのシステムからのデータが動かぬ証拠となることは容易に想定できますが、それがおとりまたは誤判定である可能性もあります。 アイルランド国家警察部隊であるAn Garda Síochánaは、2010年以来、全米行方不明・被搾取児童センター（U.S. National Center for Missing and Exploited Child：NCMEC）からCSAMに関する情報を受け取っています。 2020年 An Garda Síochánaは、これらの照会した情報の11 %以上がCSAMではなく、内容は誤判定であり、ビーチで遊ぶこどもたちのような無害な画像やビデオであることを確認しました。[77] しかし、関連する人々の疑いが晴れたのにもかかわらず、An Garda Síochána はデータを削除しませんでした。 An Garda Síochánaのファイルあるいは世界中の他の法執行機関のファイルに、CSAMの共有の疑いが晴れた人々が何名残っているかはわかりません。

結論

暗号化は、オンライン通信の保護、言論の自由の実現、金融取引の保護など、データのプライバシーとセキュリティにおいて重要な役割を果たします。 暗号化に反対する歴史的な議論は、攻撃者が同じ機能にアクセスするのを防ぎながら、機密データを保護したいという要望によって特徴づけられてきました。技術は進化し続けていますが、「暗号化の議論」は停滞しています。議論を前進させるには、話し合いを再考し、漸進的な進歩がイノベーションの鍵であることを受け入れる必要があります。

例外的なアクセスは、CSAMやその他の犯罪を解決する唯一の方法として宣伝されてきましたが、これは本質への注意をそらすものです。真の問題は犯罪そのものであり、暗号化や技術ではないのです。 Center for Cybersecurity Policy & Law、および大多数のサイバーセキュリティコミュニティは、暗号化を弱めることはすべての組織と個人のセキュリティ、プライバシー、自由権、および重要な社会的利益を危険にさらすと考えています。法を順守する市民のプライバシーを保護しながら、これらの犯罪を解決するための他の解決策や方法も存在します。 これらのアプローチは、戦略国際問題研究所（CSIS）、カーネギー国際平和基金、プリンストン大学、国際技術政策センターによって提唱されています。 段階的な進歩に向け我々の焦点を転換することが不可欠です。

---

[76] Ibid

[77] https://www.iccl.ie/news/an-garda-siochana-unlawfully-retains-files-on-innocent-people-who-it-has-already-cleared-of-producing-or-sharing-of-child-sex-abuse-material/