(Accessnow)暗号化を攻撃することで誰が傷つくのか

2021 年 10 月 21 日 | 午前 12 時 30 分

ニュースでは、法執行機関が私たちの暗号化された通信へのアクセスを要求していることを示す記事がたくさんある。犯罪者やテロリストが暗号を使用しているため、そのようなアクセスが必要だと主張している。しかし、それは話の一面に過ぎない。

暗号化は、法執行機関が標的としている犯罪者から私たちを守るためのものでもある。暗号化は、人権擁護者を強力な敵から守るための重要なツールでもある。また、基本的なオンラインの安全性、安全な取引や通信にも欠かせない。また、民主主義を存続させ、国連が定めた人権を守るためにも欠かせない。

人間として、私たちは皆、個人的で私的な会話をオンライン上で支障なく行う自由を必要としている。しかし、強力な暗号化は、さらに緊急性の高いニーズに応えるものだ。人権擁護者にとって、暗号化は生死を分けるものだ。だからこそ、暗号化に関するいかなる政策も、彼らの重要な仕事が損なわれないようにしなければならない。もし、暗号化を弱めたり、迂回させたりして、コミュニティの中で最もリスクの高い個人や組織を保護できなければ、より多くの人々が殺され、重要な人権活動が損なわれることになる。

現在、COVID-19 では、私たちの活動の多くがオンライン化されており、人権派弁護士とそのクライアント（人権侵害の被害者）との間で交わされる会話など、機密性の高い会話がインターネット上で交わされている。このような会話の秘密を守ることは必須だ。

Access Now のデジタル・セキュリティ・ヘルプラインでは、より安全な世界を実現するために暗号化が不可欠であることを示す事例を扱っている。以下に 5 つの事例を紹介する。なお、安全を確保するために、団体名や個人名、身元が漏れる可能性のある情報は変更または省略してある。

事例 1：ニカラグアの総選挙を前に、暗号化によって市民社会が監視、脅迫、投獄から守られる

ニカラグアのいくつかの市民社会団体は、当局が自分たちの音声通話や SMS メッセージを監視しているのではないかと強く疑っている。私たちのヘルプラインは、彼らの通話やメッセージが傍受されないように、機密性の高い通信をエンドツーエンドで暗号化されたメッセージングプラットフォームに移行するための支援を行っている。

これは緊急かつ必要な作業だ。ニカラグア国民は、2021 年 11 月 7 日の総選挙の投票を控えているが、この選挙に向けて、ほとんどすべての政治的反対活動や人権活動が犯罪化されている。野党の政治家や人権擁護者に対する監視や脅迫は、国中に蔓延している。逮捕されたり、不当に長く投獄されたり、さらに悪い状況に直面しているだけでなく、多くのニカラグアの人々は脅迫による萎縮効果によって自主検閲をするようになっている。

ケース 2：腐敗した政権下で、暗号化によって調査報道記者や情報提供者を報復から守る

危険な環境にある国で腐敗の摘発に取り組んでいる組織が、仕事用と個人用のデバイスで受信したり保存したりする情報を保護するために、ヘルプラインの支援を求めてた。腐敗防止のための調査は、個人や組織にとって最も危険な種類の仕事の一つだ。加害者は通常、大きな権力を持っており、その権力をフルに活用して腐敗行為が明らかになるのを防ごうとする。そのため、記者や情報提供者は、脅迫から殺人に至るまで、あらゆる場面で標的となる。

今回のケースの組織は、腐敗の摘発、選挙の監視、人権と政府の説明責任の促進を目的としている。問題の国では、市民社会が攻撃を受け、ジャーナリストが殺害され、過激派グループがNGOを脅迫している。そのため、私たちのヘルプラインは、強力な暗号化を使用して、汚職事件に関連するすべての機密データを保護するために組織を支援した。

事例3：地中海を渡る難民・移民のSOSコールを暗号化で安全に守り、Alarm Phoneが命を救う

Alarm Phoneは、地中海を渡る難民・移民の緊急支援を目的とした自己組織化されたホットラインだ。ヨーロッパと北アフリカの市民社会のボランティアによる国境を越えたネットワークによって運営されているAlarm Phoneは、SOSコールに注意を喚起し、発生した事件を記録し、沿岸警備隊に連絡し、必要に応じて追加の救助支援をリアルタイムで動員する。Alarm Phoneは、重要な人権保護活動を促進し、人命を救う。私たちのヘルプラインは、その通信手段の確保を支援した。

強力な暗号化により、Alarm Phoneが活動する場所によっては、リスクが軽減される。一部の国では、政府が移民や難民を支援する団体を人身売買の疑いで取り締まっている。また、移民に反対する極右団体からのリスクもある。Alarm Phoneの通信を安全に保つことで、その活動が犯罪者扱いされたり、スタッフが嫌がらせを受けたりするリスクを減らすことができる。

ケース4：人身売買の捜査で、暗号化により情報提供者を組織犯罪者から守る

ある人身売買対策団体は、非常に機密性の高い人身売買調査のデジタル記録を安全に保存する方法を知りたくて、私たちのヘルプラインに問い合わせてきた。保護すべきデータには、情報提供者の詳細も含まれていた。人身売買を行う犯罪者が、この組織の通信を傍受して情報提供者を特定した場合、情報提供者や法廷での証人候補が殺害の対象になるなど、深刻な事態に陥る可能性がある。

ケース5：LGBTQ+の活動家がソーシャルメディア・プラットフォームを利用する際に、強力な認証で侵害や攻撃を防ぐ

暗号化は、機密性の高い通信の秘密を守るために必要なだけではない。また、暗号化は、人権擁護者がオンラインで安全に活動するために不可欠な、強固な認証を確保することもできる。

私たちのヘルプラインは、南アジアのLGBTQ+活動家がソーシャルメディアのアカウントを保護するために、暗号化されたハードウェアトークンを使用した多要素認証の設定を支援した。活動家の活動に反対する攻撃者は、ソーシャルメディアのアカウントを侵害して活動を妨害したり、連絡先やネットワークを特定したり、あるいは活動家になりすまして誤った情報を広めたり評判を落としたりすることがよくある。

私たちのオンラインコミュニケーションは、最も弱い環の安全こそが安全を意味する。暗号化を弱体化させようとする政府や、暗号化を回避するシステムを開発する企業は、私たちの安全を守る鎖を引っ張っている。しかし、これらの事例が示すように、強力な暗号化は、人権擁護者にとって極めて重要だ。

暗号化についての決定は、CSAMの拡散をコントロールするような、イデオロギー的には善意のイニシアティブのためのメカニズムの開発も含めて、いわゆる平均的なユーザーのニーズに基づいてなされるべきではない。民主主義、権利、自由の未来を形作る変革者や人権擁護者など、最もリスクの高い人々への影響を十分に理解した上で決定すべきだ。

出典：https://www.accessnow.org/who-we-hurt-when-we-attack-encryption/

公開書簡:犯罪行為を防止しつつプライバシーを守るための市民社会の見解

2020年10月27日
公開書簡。犯罪行為を防止しつつプライバシーを守るための市民社会の見解
拝啓 ウルスラ・フォン・デア・ライエン欧州委員会委員長
親愛なるイルヴァ・ヨハンソン委員。

ティエリー・ブルトン委員へ
CC. 欧州委員会委員長 ビヨーン・セイベルト内閣総理大臣、デジタル委員会委員長
顧問アンソニー・ウィラン、ブルトン委員長ムタリエ、ヨハンソン委員長オーサ・ウェバー、トム・スネルス内閣府副長官。

我々、以下の団体は、児童性的虐待資料（Child Sexual Abuse Material CSAM）とのより効果的な戦いのための EU 戦略に関するコミュニケーションと、e プライバシー指令を改正する暫定規則と内部討議文書「エンドツーエンド暗号化通信における児童性的虐待を検出するための技術的ソリューション Technical solutions to detect child sexual abuse in end-to-end encrypted communications」を含む、そこから派生する提案について、我々の見解を皆様と共有したいと思います。この書簡では、提案の一部に対する**我々の懸念**を強調するとともに、これらの文書から派生する政策イニシアチブにおいて、**プライバシー、データ保護、その他の基本的権利が尊重されることを確保し、公開協議や公開会議を通じて市民社会の有意義な参加を確保すること**を要請します。

署名者は、子どもを保護するという欧州委員会の目標を共有しています。児童の性的虐待は、被害者にとって極めて深刻な結果をもたらす重大な犯罪です。**オンラインでもオフラインでも、子どもに対するあらゆる形態の暴力を効果的に排除しなければなりません。**この目標を達成するための多くの効果的な手段は、公教育や被害者支援から国境を越えた警察の協力の改善に至るまで、テクノロジー以外に見出すことができると思われます。我々は、指令 2011/92/EU の多くの側面を加盟国が確実に遵守するための欧州委員会の作業プログラムを歓迎します。現在、多くの CSA ウェブサイトは欧州でホストされており、我々は、欧州委員会がクライアント側のフィルタリングよりも、この非技術的な作業と、違反ウェブサイトの迅速な削除を優先させることを提案します。

我々は、**前述の 3 つの文書がもたらす 5 つの基本的権利の問題に焦点を当てたい**と思います。

対象となるサービスの明確性の欠如と、現在の慣行の法的根拠の欠如

我々は、使用される技術が「業界の最新技術に基づき、プライバシーへの干渉が最も少ないものであるべきであり、テキストを含む通信の系統的なフィルタリングやスキャンを含まず、児童性的虐待の疑いの具体的な要素がある場合にのみ特定の通信を調査すべきである」とした暫定規則の説明文 11 を歓迎します。しかし、欧州委員会が CSAM を検知するための「個人データその他のデータを処理するための技術」を対象にすると述べた際に、どのような具体的なサービス、プラットフォーム、アプリケーション、技術に言及しているのか、また、サービス、プラットフォーム、アプリケーション、技術を提供する企業がどのような法的根拠に基づいて（もしあれば）現在これらの慣行を実施しているのかは、完全には明らかではありません。(注 1)

影響評価と重要な協議の欠如

私たちは、基本権庁（FRA）、欧州データ保護監督官（EDPS）、人権団体からの公開協議、影響評価、専門家の意見募集が完全に欠如していたことを遺憾に思います。欧州電子通信規約 European Electronic Communications Code の発効を考慮してスケジュールを急ぐという現在の正当化の理由は、基本的権利への潜在的な影響を考慮すると受け入れられません。

例外的措置の正常化

我々は、中間規則の措置が一時的なものであるという主張を認めます。しかし、中間規則の適用期間は 2025 年まで続くことに留意し、一旦採択されれば、中間規則が奨励する一時的な措置が認められた慣行となり、それが無条件に共犯として更新されてしまうことを懸念しています。このような例外的な法律が新たな規範として受け入れられるようになる危険性は深刻です。

大手テクノロジー企業への権限移譲

これらの文書で提案されている措置のいくつかは、基本的権利に影響するため、公的機関の責任であるべき監視や検閲の仕組みを民間企業に任せることになります。この点に関して、我々は、CSAM を検出するためのハッシュマッチング技術を含むあらゆるフィルタリングメカニズムが人権に与える影響を慎重に検討することを欧州委員会に奨励します。**違法な素材を検出するためにハッシュデータベー**

スを使用する将来のイニシアチブは、基本的権利の保護を含む強力な法の支配の枠組みの中で追求されなければなりません。そのためには、このようなデータベースがオープンソースのソフトウェアで運営され、公的な独立機関によって管理され、米国の組織が扱う米国の技術やデータベースに頼るのではなく(注 2)、**完全な公的な監視下で運営されていることを保証すること**も含まれます。(注 3)

暗号化に対する潜在的な攻撃

Ðer Spiegel(注 4)が調査したように、「Technical Solutions」のディスカッションペーパーで推奨されている提案のいくつかは、メッセージが暗号化されて送信される前に、外部サーバーの助けを借りて、ユーザーのエンドデバイス上のメッセージを事前にフィルタリングすることで構成されているため、事実上、エンドツーエンドの暗号化を破壊することになります。これは、EÐRi が以前の専用ページやドイツ大統領府への最近の書簡で表明したように、暗号化の重要な技術的保護機能を損なうものです。(注 5)

特に、技術的解決策に関する文書は、少なくとも 2 つの点で技術的に欠陥があります。第一に、「プライバシー」に対するさまざまな技術的解決策を評価していますが、この用語を定義できていません。第二に、この文書が特定している好ましい解決策はすべて、法執行機関がコンテンツへの例外的なアクセスを得るという結果を伴うものでありながら、他方で受信者がエンドツーエンドで暗号化された通信を受信して復号化するという結果を達成するとも主張しています。この 2 つの結果は矛盾しています。サービスを介して共有された通信の送信者と受信者だけがそのコンテンツにアクセスできない限り、サービスはエンドツーエンド暗号化によって完全に保護されているとはいえません。

私たちは、欧州委員会に対し、プライバシー、表現の自由、およびこれらの権利を侵害した場合の効果的な救済手段を利用する権利を含む子どもの権利の全範囲を検討するよう強く求めます。

暗号化は、子どもたちの機密情報を確実に保護することで、子どもたちに利益をもたらします。ユニセフが認識しているように、子どもたちのプライバシーと データ保護を改善することは、子どもたちの発達と大人となる将来にとって不可欠である。ユニセフは、あらゆる監視ツールが「表現と情報の権利を行使する子どもたちの自律性の成長を念頭に置く」 ことを求めています。(注 6)
ユニセフが強調しているように、監視に関する国内法は、プライバシーの権利を含む国際的な人権規範を遵守しなければなりません。実際には、政府による通信データの要求は、司法的に認可され、対象を絞り、合理的な疑いに基づき、正当な目的を達成するために必要かつ比例したものでなければならないことを意味します。国際人権法の下では、暗号の使用を制限するような措置は、通信データの大量傍受や全面的な保持と同様に、深刻な問題を孕んでいます。

子どもの権利に意味のある影響を与えるために、私たちは、**欧州データ保護監督機関(EÐPS)**と**基本的権利庁(FRA)**からの意見によって情報を得られるように、これらの提案に関する議論を要求します。さらに、私たちは、公開討論に加えて、この書簡で議論された文書から派生するさまざまな提案についての適切な**影響評価**とともに、公開での協議を準備することを要求します。最後に、**市民社会のグループ、特に子どもの権利のグループだけでなく、人権とデジタルの権利の組織も参加**し、受け入れ可能な法的解決策を見つけるために協力する必要があります。こうした条件を満たさないのであれば、必ずしも子どもたちを保護するものではなく、子どもたちを含むすべての人たちのプライベートなコミュニケーションを、大量監視の対象とする可能性が高くなります。

私たちは、この書簡で取り上げられた問題について、皆様と議論することを楽しみにしています。

敬具
ディエゴ・ナランジョ 政策責任者欧州デジタル著作権 (EÐLi

(訳注) PhotoÐNA
「PhotoÐNA とはマイクロソフトが開発した技術で、類似する画像を識別するために画像のハッシュ値を計算する。現在同社のサービスである Bing、OneÐrive だけでなく、Google Gmail、Twitter、Facebook、Adobe Systems、National Center for Missing and Exploited Children で採用されている。

主に児童ポルノの流通阻止の為に使用されており、画像のハッシュを計算することで検出している。このハッシュはサイズが変更されていたり、目立たない配色変更を含む画像の変更があっても変更されないように計算されている[1]。PhotoÐNA は画像を白黒化し、サイズを変更し、格子状に分割し、輝度勾配や輪郭を探索している。」
https://ja.wikipedia.org/wiki/PhotoÐNA