政策立案者向けのためのファクトシート：

「合法アクセス」によるセキュリティリスク — 6つの理由

暗号化とは？

暗号化とは、情報をスクランブルまたは表示できないようにして、元の状態に戻すための手段（または鍵）を持っている人だけが読むことができるようにするプロセスです。**エンドツーエンド（E2E）の暗号化によって、最強のセキュリティと信頼度を実現できます。**理想的には、メッセージを復号化するための鍵は、本来の受信者だけが持つことになるからです。第三者は鍵を持っていません。

暗号化技術は、デジタルデータと通信の完全性と機密性を保護することで、オンライン上のユーザーを安全に守るためのツールです。これによりWeb閲覧、オンラインバンキング、電力、選挙、病院や輸送などの重要な公共サービスと、それに依存している市民一人ひとりの安全性を確保できます。2018年には17億人以上のユーザーが、E2Eの暗号化メッセージングサービスで通信を保護しました。[1]

一部の行政機関は、暗号化によって、テロ、犯罪の防止や懲罰のための情報収集が難しくなるのではないかと懸念しています。そして急いで**「合法アクセス」規制**を定め、警察や諜報機関に、暗号化された通信の傍受やアクセスのための権限を与える、あるいは企業にそれを依頼しています。**これはオンライン上のあらゆる人々にとって危険なことです。**

こうした規制は暗号化に影響がなく、別な方法でアクセスできるという意見もありますが、ユーザーセキュリティのリスクがあります。セキュアなサービスへのあらゆるエントリーポイントが脆弱になってしまいます。

「合法アクセス」はインターネットのセキュリティを低下させ、世界経済、私達が依存している重要なサービス、すべての市民生活のリスクを増大させます。その理由は以下のとおりです。

1. **強制的にセキュリティを低下させることで、私達すべての脆弱性が高まる：**「善良な市民」だけが開けられて、「悪者」には開けられないようなデジタルロックはありません。「合法アクセス」によって、犯罪者や敵意のある行政機関など、本来意図していない相手が機密データを簡単に入手できるようになります。

2. **国家の安全と個人の安全性に関するリスク：**個人情報、銀行データ、国の機密のセキュリティを低下させることで、「合法アクセス」は意図せずにスパイ行為、なりすまし、ブラックメール、市場操作などを促進する可能性があります。

3. **テロリストの新たな隠れ蓑：**テロリストと犯罪者が、警察が暗号化メッセージサービスにアクセスできるようになったことを知った場合、別な方法を使用するようになるでしょう。その結果、犯罪者やテロリストの通信が監視対象から外れ、一般のユーザーの脆弱性が高まってしまいます。

4. **人命に関わる：**エンドツーエンドに暗号化された通信により、ジャーナリスト、活動家、身柄を保護された証人、覆面警官、その他大勢の人々の身元が保護されます。脆弱な通信によって、これらの人々の命が危険にさらされます。

5. **インターネットインフラストラクチャのリスク：**「合法アクセス」によって、オンラインでの日々の安全性確保に欠かせない認証メカニズムなど、インターネットインフラストラクチャレイヤーの主要なセキュリティコンポーネントが危険にさらされます。

6. **取引や投資への影響：**「合法アクセス」は、世界経済に大きな影響を及ぼす可能性があります。ほとんどの多国籍企業は、海外の新興市場で売上の多くを得ており、ビジネスの潜在的な成長もかなりの部分をこうした市場に依存しています。人々は、行政機関が機密情報や通信にアクセスできる国からの製品購入やサービス利用は避けようとします。

[1] https://telegram.org/blog/200-million; https://techcrunch.com/2018/01/31/whatsapp-hits-1-5-billion-monthly-users-19b-not-so-bad

どの国にも市民を守る権利と義務があります。ただし、善良な意図であったとしても、安易にアクセスを促そうとする試みは法を順守している市民や、インターネット全体のセキュリティを著しく脅かす危険性があります。

私達の国、経済生活、そして自分自身を守ってくれる、最も強力なデジタルツールを取り上げないでください。すべての人々にとっての強力な暗号化に対応するよう、世界中のリーダーに訴えかけましょう。

Internet Society internetsociety.org