

欧州におけるエンド・ツー・エンド暗号化規制の試み

○八田真行 (Masayuki Hatta)

Keywords : エンド・ツー・エンド暗号化、クライアントサイドスキニング、プライバシー、サイバーセキュリティ、技術規制

1 目的

近年、欧州では児童保護やテロ対策を名目として、エンド・ツー・エンド暗号化(E2EE)に対する規制強化の動きが顕著になっている。英国のオンライン安全法、EUのチャット・コントロールなど、複数の法制度が暗号化通信へのアクセスを求める条項を含んでいる。本研究は、これら欧州諸国におけるE2EE規制の試みを包括的に調査し、その政策的意図、技術的影響、そしてプライバシーとセキュリティへの波及効果を明らかにすることを目的とする。特に、善意の政策目的が技術的実現可能性や基本的人権とどのように衝突しているかを分析する。

2 方法

本研究の調査・分析手法は主に文献調査である。具体的には、英国オンライン安全法、EUのチャット・コントロール案、各国の関連法案の条文分析を行うとともに、欧州議会や各国議会での議論記録を精査した。また、暗号研究者、セキュリティ専門家、プライバシー擁護団体による技術的評価レポートや声明を収集・分析した。さらに、主要なテクノロジー企業の公式見解や対応方針についても文献調査を実施し、規制案が実際の技術実装に与える影響を評価した。

3 結果

調査・分析の結果、欧州各国の規制案には共通して、暗号化通信の内容へのアクセスを可能にする技術的措置を求める条項が含まれていることが判明した。英国オンライン安全法では、Ofcomが技術的能力命令を発行できる権限が規定され、EUのチャット・コントロールではクライアントサイドスキニング(CSS)の実装が事実上要求されている。セキュリティ専門家からは、これらの措置がE2EEの根本的な安全性を損なうという強い懸念が表明されている。バックドアやCSSの導入は、意図された犯罪捜査目的だけでなく、悪意ある第三者による悪用リスクを大幅に高めると指摘されている。また、複数のテクノロジー企業が、このような規制が施行された場合、欧州市場からのE2EEサービス撤退を検討していることが明らかになった。

4 結論

あるセキュリティ研究者は、オンライン安全法を評して「well-intentioned disaster (善意から生まれた災難)」と表現している。これは、近年の欧州の暗号規制全体に当てはまる評価である。児童保護という正当な政策目標が、技術的実現可能性や包括的セキュリティへの影響を十分に考慮しないまま法制化されようとしている。ポピュリズムの勃興と相まって、ネット規制の動きが強まる中で、民主主義社会における基本的な通信の秘密とデジタルセキュリティの基盤が脅かされることが懸念される。政策立案者は、短期的な政治的成果を求めるあまり、長期的なサイバーセキュリティ環境の悪化という代償を見過ごしてはならない。

【主要参考文献】

Harold Abelson, et. al. Bugs in our pockets: the risks of client-side scanning, *Journal of Cybersecurity*, Volume 10, Issue 1, 2024, tyad020, <https://doi.org/10.1093/cybsec/tyad020>