「テロリストによる暗号通信の実態に関する一考察」
–世界の治安・情報機関も解読できず–

安部川元伸[†1]　岡田　忠[†2]

概要：アルカイダの全盛期からテロリストは暗号通信を行い，治安・情報機関によるテロ計画の探知と工作員の事前摘発を免れようとしてきた．特に,2013 年に米国家安全保障局のエドワード・スノーデンが米国による通信傍受の全容を暴露したことで，テロリスト側も作戦を変更し，暗号による情報のやり取りをさらに重視するようになった．コンピュータやスマートフォンの急速な発達で，通信者のプライバシーが厳重に保護されるようになり，捜査機関が暗号通信を傍受してもその解読が不可能になっている．公共の安全とプライバシー保護という対極の概念をめぐる口角泡を飛ばす論議は，今後も静まることはないだろう．

キーワード：テロリスト，メッセンジャー，アプリケーション，暗号化，秘匿通信，アルカイダ，イスラム国,

A Consideration on the Picture of Terrorists' Encrypted Communications
～Unable to Decode Even by Security and Intelligence Agencies in the World～

MOTONOBU ABEKAWA[†1]　TADASHI OKADA[†2]

Abstract: Since it's golden age has been continuing, Al Qaeda has used the method of encrypted device for their secret communications in order to avoid authorities' monitoring on terror planning and disruption of terrorists' dangerous activities before carrying out their terrorist attacks. Followed by the disclosure through the leak of Edward Snowden, a former CIA agent, particularly, of the whole picture of the NSC's eavesdrop operation against the world, then terrorist organizations had to change their ways of communication to transfer clandestine information with being stringently encrypted. As rapid development in computer or smartphone technology as sophisticated communication tools, on the other hand, privacy and human rights became further protected than before, which caused security and intelligence agencies driven into the serious trial ground because even those were unable to decode terrorists encrypted message. Now, intense discussion is made between advocates of one side, securing public safety, and the other, protecting man's privacy, which might never be declined.

Keywords: Terrorist, Messenger, Application, Encryption, Secure Communication, Al Qaeda, Islamic State

1. はじめに

シリアとイラクにおける過激派組織，「イスラム国」の拠点が次々に陥落している中で，欧州，米州，アジアなどの先進国におけるテロが頻発するようになっている．2014 年 6 月にカリフ国家建設を宣言した「イスラム国」に憧れ，世界中から何万人といわれる外国人戦士がシリア，イラクに渡ったといわれる．しかし，最近の両国では，「イスラム国」の敗走が続き，組織自体が崩壊の危機に瀕していることから，彼らの一部が続々と出身国に帰国し，母国での報復テロの機会を狙っているとみられている．こうした外国人戦士や「イスラム国」に影響を受けた先進国に住む過激分子たちは，テロ訓練で先進国の治安・情報機関の捜査手法を研究し,捜査をすり抜ける方法を熟知しているため，テロの事前摘発は，ますます困難になっている．その最大の理由として考えられることは，テロリストが解読不能な暗号システムを使用し，メンバー間，細胞間の連絡に活用していることが挙げられる．国際社会もテロリストの暗号使用を規制しようと様々に働き掛けてはいるが，通信の秘密など，プライバシーの保護の問題が足枷となり，状況は必ずしも楽観できるものではない．そのため，テロリストが使用しているメッセンジャー・アプリケーションを考察する．

2. 先行研究

テロリストのコミュニケーションについての研究は実施例が少なく先行研究例の発見には困難を伴う．その中でテロとコミュニケーション，メッセージなどの関連のあるキーワードで抽出した研究を参考までに記述する．[1]永田らの研究では，アトランタオリンピック開催中に爆弾テロが発生した際に対応するためのリスクコミュニケーションについて記述されているが，[2]小川原の研究では，テロリストのプロファイリングを行い，テロリストを見分ける研究であるが，テロリスト同士の連絡のやり取りの手法など

†1 日本大学 危機管理学部 College Of Risk Management ,Nihon University
†2 茨城大学大学院 理工学研究科 Graduate School of Science and Engineering ,Ibaraki Univ.

の研究は行われていない．[3]福田の研究では，報道におけるテロに関するマスメディアのコミュニケーションについての研究であり、テロリスト同士のコミュニケーションについては触れていない．[4]中村の研究では，テロリストがどのような手法と行動をおこなってテロを行うのかを考察しているが，テロリストのコミュニケーションの手法には触れていない. いずれの研究でもテロリストの IT を活用したコミュニケーションや秘匿メッセージを行うためのツールの研究は行われていない．他，本テーマに関連した調査研究は，[5]から[8]などが参考になる．

3. テロリストが本格的に暗号通信を行うようになったのはアルカイダから

テロリストの使命は，テロ計画を警察に事前察知されることなく, 確実に成功させることであろう. アルカイダは, コンピュータ，モバイルの飛躍的な発達に目をつけ，こうした技術を早くから導入してきた．組織のカリスマ的指導者であったオサマ・ビン・ラディン（以降、ビンラディン）は, 大の IT 好きであり, しかも, 極めて慎重な性格のため，暗号処理された電子メール，電話を多用していたといわれる．

図 1 ウサマ・ビン・ラディン

しかし，米国の無人機による攻撃で，幹部が次々に死亡するなど，組織の通信が敵に盗聴されているとの確信を抱いたビンラディンは，衛星携帯電話や PC によるインターネット通信を一切中止した．代わりに，ビンラディンは一切の連絡を信頼の置ける腹心の部下のみに命じ，直接面会して指示を直接相手に下すことにした．アルカイダのクーリエは，単に最高幹部の指示・命令を伝えるだけでなく，現金の搬送も受け持っていたといわれる．

アルカイダは, 9.11 米国同時多発テロでも暗号通信を使用していた．当時話題になっていたのは，画像にメッセージを隠し電子処理して送付する「ステガノグラフィー＊a」や「デジタル透かし」(Digital Watermarking)などであった．

＊a ステガノグラフィー(steganography)とは，データ隠蔽技術の一つで，データを他のデータに埋め込む方式．暗号化したことが一見わからないようにするもの

4. メッセージの秘匿

「デジタル透かし」(Digital Watermarking)とは，紙幣の透かしとは異なり見た目には分からないが，検出ソフトを使用することによって，埋め込まれた情報を取り出すことができる．不正コピーやデータ改竄の検出など，主に著作権保護の用途に使われることを想定した研究開発が続けられている．情報を埋め込むコンテンツとしては，テキスト，画像，音声，動画，プログラムなどがある．なお，ステカガノグラフィー(Steganography)は，あくまで通信の隠匿が目的であり，コンテンツは情報を隠す媒体でしかない．

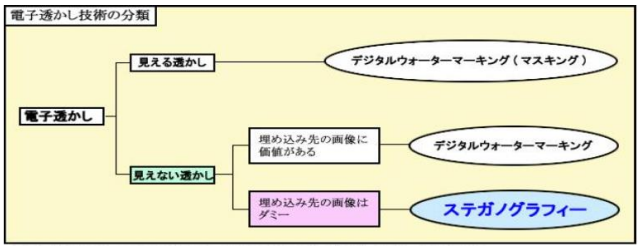

図 2 電子透かし技術の分類
出典: Inside of Garage

図 3 電子透かし（知覚可能型）の例
出典：Visible digital watermarking. Wikimedia Commons

5. ステガノグラフィーの実例

図 4「シェイクスピアの画像を利用した例」では，人間の視覚での認識はできない．そのため比較しても，両者の違いは肉眼では判別できない．

右側のシェイクスピアの肖像画に隠されているメッセージは，“Bin Laden Determined to Strike Inside US”である．

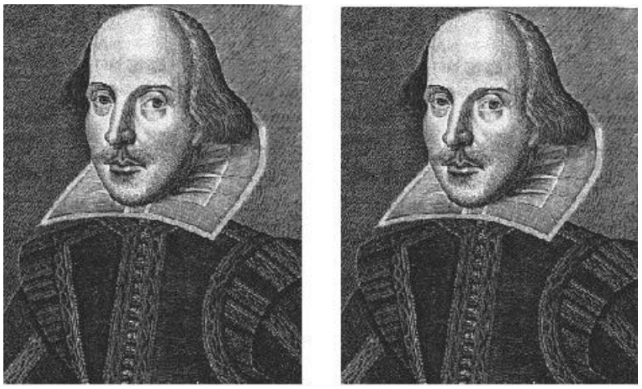

図 5 シェイクスピアの画像を利用した例
出典: Neil F. Johnson. Steganography. Technical Report. November 1995.

6. アルカイダが開発した暗号システム

アルカイダは，9.11 テロ以降から独自の暗号システムを開発し，厳しい米国やその同盟国による追及をかわし，組織間の通信をより安全に行うようにした．「アラビア半島のアルカイダ」(AQAP)のウェブ・マガジン，図 6「インスパイア 2010 夏号暗号掲載の使用法」では，アルカイダのメンバーや影響を受けている人々に対して，暗号の使用法を掲載することで秘匿性を持ったメッセージのやり取りを指南している．

アルカイダは，容易に通信ができるように暗号化などを用いて，通信の秘匿性を確保したコミュニケーションをおこなうために，アルカイダが既存のシステムをカスタマイズして使い勝手を良くしたツールがある．

アルカイダが実際に使用していた暗号システムを下記に記述する．

■ Mujahideen Secrets(Asrat al-Mujahideen):暗号化ソフト
アルカイダが 2007 年から頻繁に使用．携帯電話，マッキントッシの PC から発信する電子メールをサポート

■ Asrar-al-Dardashah アルカイダのイスラム主義宣伝組織「Global Islamic Media Front」 (GIMF)が 2013 年 2 月に公表．主にインターネットを通して利用されるインスタント・メッセージを中心に扱うコミュニケーション用アプリ．米国メンバーとの通信に多く使用された

■ Tashfeer al-Jawwal
GIMF が 2013 年 9 月に公表した携帯電話，スマートフォン用の OS である Synbian と Android 用に開発した携帯電話用の暗号プログラム

■ Asrar al-Ghurabaa
IS が 2013 年 11 月に公表した暗号．IS がアルカイダ中枢からの分裂後に独自に使用し始めた

■ Amn al-Mujahid
アルカイダ配下の FTC(アル・ファジール技術委員会)が 2013 年 12 月に公開した補助的な暗号プログラム

図 7「インスパイア 2010 夏号」掲載暗号の使用法

7. 9.11 事件以降，通信傍受により事前摘発されたテロ事件

9.11 事件以降の通信傍受によって，未然にテロ事件を摘発し，防ぐことができたテロ事件の事例を下記に記述する．

■ 英国-北米間旅客機同時自爆テロ未遂事件(2006 年)
2006 年に発覚した英国発米国・カナダ行きの旅客機 7 機に対する同時自爆テロ未遂事件．犯人の 8 人は，ヒースロー空港から米国及びカナダ行きの各便に飲料用ボトルに入れた液体爆弾を持ち込んで自爆する計画を立てていた．

■ アルカイダのドイツ同時多発テロ計画(2007 年)
アルカイダの影響を受けて過激化した 3 人（ドイツ人 2 人，トルコ人 1 人）がドイツ国内の米軍施設とラムシュタイン米空軍基地に対して大規模な爆弾テロを計画したが事前に摘発．

■ 米ニューヨークの地下鉄爆破計画(2009 年)
パキスタンのアルカイダ訓練キャンプでテロ訓練を受けた米コロラド州居住のアフガニスタン人ナジブラ・ザジ容疑者がニューヨークの地下鉄爆破を計画．

これらのテロ計画が摘発されて以降，アルカイダは，暗号通信をより重視するようになった．

8. エドワード･スノーデンの暴露事件以降の動向

2013 年に NSA（米国家安全保障局）の契約雇員エドワード・スノーデン（元 CIA 職員）が，アップル，グーグル，フェイスブック，マイクロソフトなどの IT 企業が提供するネットサービスのサーバーに NSA が直接アクセスし，ユーザーのデータを収集していたことを暴露した．盗聴の標的には，ドイツのメルケル首相の携帯電話も含まれていたことが発覚し，大きな波紋を投げかけた．

この事態を受け，アルカイダ，IS などのテロ組織も急遽，通信方法の変更を迫られた．アルカイダを中心とするテロ組織は，電子メールのアカウントや携帯電話のプロバイダーを即座に変更し，同時に新しい暗号技術の導入を決めた．

さらに，新たにリクルートしたメンバーに対し，チャットやウェブを見る際には，自分の本当のアドレス，電話番号などを決して使用せず，Skype も傍受の可能性が高いツールとして使用中止を徹底した．

テロリストは，スノーデンの発言から，GPS を活用した PC の位置情報を NSA に追跡されないよう注意（特殊なオンライン・ソフトウェアを使用）し，関連する機材を配布した．

NSA のアレクサンダー長官（当時）は，スノーデンのリークは取り返しのつかない大失態であり，国家が被ったダメージは極めて重大であると発言した．

9. イスラム国が使用している暗号システム

- END-TO-END ENCRYPTION (E2EE)

E2EE の代表的ソフトに，PGP (Pretty Good Privacy)があるが，これは極めて高度な暗号技術であり，解読は事実上不可能に近いとされている．「共通鍵暗号方式」と「公開鍵暗号方式」の 2 種類の暗号化方式を併用し，高速で安全なデータの暗号化通信を実現したシステムである．秘密鍵を使用しないと解読はできない．重要通信には必須のツールである．

なお、「イスラム国」の大方のメンバーは、現在，機動性に優れたスマートフォンを多用しているが、同組織が使用しているスマートフォン用の暗号化メッセンジャー・アプリケーションを下記に列記する．

- KIK
  スマートフォン，Android，Windows の電話システムに使用できるカナダ製の無料アプリ．使用者の匿名を守る．
- SURESPOT
  安全な携帯用の暗号メッセンジャー．送信されたメッセージは，宛名の人物しか見ることができない
- WICKR
  米国サンフランシスコの企業が開発した無料の E2EE ソフトで極めて信頼度が高い
- TELEGRAM
  パリ同時多発テロの容疑者の 1 人が捨てた携帯電話に攻撃の 7 時間前に TEREGLAM がインストールされていた．メッセージは厳重に暗号化され，送信速度が速いのが特徴．通信内容を自動的に消去できる．使用者数は世界に 1 億人といわれる
- WhatsApp (有料)
  全世界 180 か国で使われ，使用者は 10 億人を超える

これらの暗号メッセンジャー・アプリケーションの特徴は，メッセージの送信後，一定時間が経過すると送信したメッセージが自動的に削除されるように設定することができることである．通信の痕跡を残さないため，情報機関の追跡を避けることができる．いずれも既存の商業用システムであり，操作が簡単でしかも安全性が高い．

10. 世界の治安・情報機関の対応

パリ同時多発テロ（2015.11）後，米アップルとグーグルはスマートフォンの暗号解読手段を当局に提供するよう要請された．さらに，FBI 長官は，議会公聴会で，「イスラム国が SNS で要員の募集を行い，めぼしい者を見つけたら，ツイッターのダイレクトメッセージに切り替えて暗号での交渉を始める．当局は，裁判所の令状があれば，その内容にアクセスできるが，2014 年にアップルとグーグルが導入した暗号機能を持つスマートフォンでは，情報にアクセスすることができない」と発言した．

しかし，これに対してグーグル社は，アップル社にも照会状を出したものの，いまのところは両社ともにコメントを控えている．

続いて，ニューヨーク州政府は，州議会に「暗号解読できないスマートフォンの販売に罰金を科すという法案を提出（2016 年 1 月）した．すなわち，同法案では，違反した業者には，端末 1 台ごとに$2,500 の罰金を科すとしている．米国のジョー・バートン下院議員も，連邦通信委員会（FCC）の公聴会の席上，IS などテロリストのウェブサイトや SNS の停止を提案（2015 年 11 月）している．

IS は，インターネットやソーシャルメディアを戦略的に活用しているが，現在の米国では，インターネットの中立性規則や表現の自由の問題もあり，こうしたテロリストのウェブサイトを停止することはできないというのが一般的見解である．

11. 人々の安全とプライバシー保護の問題 世界の主要国には，「電子通信におけるプライバシー保護法」（ECPA）（米），

「EU データ保護指令」（EU），「1989 年データ保護法」（英国），「情報処理・情報ファイル・自由に関する法律」（仏），「連邦データ保護法」（独）などによる規制があり，テロリストの通信といえども，無闇に傍受することはできない．

例えば，ドイツとフランスでは，不法の手段で録音した電話による会話でも証拠として採用されることがあるが，裁判所に認められていない電話の傍受は犯罪行為であり，刑事訴追の対象となるとしている．

一方，米国では，基本的に裁判所の令状がない限りは米国市民の通信傍受はできないとしながらも，現実には，警察や FBI は，捜査に関係しているとの理由があれば，召喚令状のみで（捜索令状は必要ない），グーグル，ヤフー，マイクロソフトや電話会社を経由する下記の情報にアクセスできることになっている．

- 電話の番号

- 電話機の所在地
- PC の IP アドレス
- 180 日以上前に送受信したメールおよび下書き文書
- オンライン上に保存しているクラウド・データ
- ソーシャルメディアへの投稿内容
- 電子メール
- 各種メッセンジャー・アプリケーションのメッセージ
- 通話情報など

英国のキャメロン首相（当時）も，暗号化通信を禁止したい意向を表明していたが，これに対し同国インターネット担当相は，「政府はアプリケーション関係者にバックドアの鍵や暗号化データへのアクセスのためのサポートの提供を求めることはない」と言明し，プライバシーの保護を緩めることはしないと確約した．

12. 考察

公共の安全の確保とプライバシー保護を含む基本的人権の尊重は，民主主義体制下の社会において永遠のテーマとして常に議論の対象となっている．しかし，テロなどによって国の法秩序が著しく損なわれ，無辜の市民の生命と財産が大いなる危険に晒されている現状に鑑みれば，テロ組織などの反社会的集団構成員の人権がある程度制限されるのは当然のことであり，実際，テロ組織や組織犯罪に対する取締りは容赦なく実施されてきた．国民の安全を守るためには、治安・情報機関による様々な形態の諜報活動も容認されるべきだと考えるが，目的をすり替えた反対論が誤った方向に世論を誘導し，挙句に国民の生命・財産を守れなくなったとしたら，それこそ本末転倒ではないだろうか．反テロ法など、本当に必要な法制であれば情勢に応じて制定していくべきであり、さらにＩＴ開発による行動認証技術（群衆の中からテロリストを探し出す）などのセキュリティ機材の早期実用化も望まれる。

13. まとめ

テロリストが無料でダウンロードできるスマートフォン用暗号アプリで作成した暗号通信は，先進国の治安・情報機関でも復号(解読)できないため，各国でテロ事件が頻発している現状下，捜査側には焦りの色が見える．

これまでに多くのテロ計画を未然に防いできたが，それは，テロリストが敢えて暗号通信を使用しなかったために警察がテロリストの通信を傍受できたケースや，暗号を使ったつもりがミスをして，平文のメッセージを送ってしまい，警察に傍受されたケースなどである．すなわち，警察は，テロリストの側のミスをひたすら待つという現実に甘んじている観がある．

しかし，警察側にもわずかながら打開策はある．暗号通信の内容は復号できなくても，送受信の時間，送信先のアドレス，GPS による衛星位置情報などのメタデータは把握できるのである．

2015 年 11 月に起きたパリ同時多発テロの直後に，フランスの治安部隊がテロリストのアジトを急襲し，テロ細胞を殲滅したが，その際の情報端緒は，テロリスト（バラクタン劇場の自爆犯）が捨てた携帯電話の残存データを解析した結果であった．これは，むしろ警察にとって極めて幸運なケースと言えるであろう．

参考文献

[1] 永田高志,長谷川学,石井正三,橋爪誠,“アトランタオリンピック爆弾テロ”，日本外傷学会雑誌 31(1)，47-51，2017

[2] 小川原正道，“欧州におけるテロ対策の現状と課題”. 武蔵野学院大学日本総合研究所研究紀要 4, 116-123, 2007-03-15.

[3] 福田充，“イスラムは，どう語られたのか？：国際テロ報道におけるイスラム解説の談話分析”. メディア・コミュニケーション：慶応義塾大学メディア・コミュニケーション研究所紀要 (Keio media communications research). No.57 (2007. 3), p.49- 65 .

[4] 中村研一，“テロリズムの定義と行動様式“. 日本比較政治学会年報 9(0), 131-152, 2007. 9, Issue 6

[5] 安部川元伸，〝国際テロリズムハンドブック“，立花書房，2015

[6] 安部川元伸，“国際テロリズム　その戦術と実態から抑止まで”，2017

[7] 棟安実治，“情報伝達のための電子透かし技術” Fundamentals Review, Vol.2 No,2 (2008.10), p53-62

[8] Robert Graham, How Terrorists Use Encryption, CTC Sentinel June 2016 Volume 9, Issue 6, p.20-25

著者紹介

安部川元伸
日本大学　危機管理学部
教授

岡田　忠
茨城大学大学院　理工学研究科
情報・システム科学専攻
博士後期課程