米国における暗号技術をめぐる動向

八山　幸司
JETRO/IPA New York

1　はじめに

コンピューターとインターネットが日常生活やビジネスに深く浸透するのに伴い、セキュリティの問題も一層重要になってきており、セキュリティ対策の有力な手法である暗号技術は、IT を支える重要な技術として様々なビジネスと社会システムの発展に必要不可欠なものとなっている。機械的な仕組みを利用して発達してきた暗号技術は、コンピューターの発達とともに強力な暗号を利用できるようになり、ビジネスやオンラインサービスの信頼性を高める役割を果たしている。一方で、プライバシー保護と情報監視のバランスの難しさから様々な議論が巻き起こり、さらに、モノのインターネット（IoT）やクラウドに対応した新しい暗号技術が必要となってきている。今号では、多くのビジネスと社会システムを守りつつも、その利用方法について様々な議論が巻き起こる米国の暗号技術をめぐる動向について紹介する。

最初に、暗号技術に関連する市場と動向を紹介する。暗号技術は様々な産業で導入が進められているが、特に、データの取り扱いに法規制のある金融や医療分野の企業が暗号技術を積極的に取り入れている。暗号技術の市場では、暗号に関連したハードウェアとソフトウェアの両方で市場の拡大が予想されており、企業のコンプライアンス向上による需要増加、価格低下による利用拡大、法規制へ対応するために暗号化に関連した製品の導入が進むと見られる。

次に、暗号に関連する事例として iPhone のロック解除を巡る動きを紹介する。連邦捜査局（Federal Bureau of Investigation：FBI）と Apple 社は、2015 年 12 月にカリフォルニア州で起きた銃乱射事件で使われた iPhone のロック解除を巡って対立し裁判にまで発展したが、暗号化が捜査の障害となりつつあった FBI は、暗号化を普及させていた Apple 社から協力を得ようとする意図があった。FBI が Apple 社に要求していた内容が、意図的にセキュリティを落とすことやバックドアの作成の強制につながるとして IT 企業は大きく反発しており、政府内からも慎重を期す声が上がったという。また、オバマ大統領は IT 企業に歩み寄りを求めており、FBI 長官も国民を含めて議論を続けていく意向を示している。一方で、連邦議会の議員からは裁判所の要請に応じて暗号解除を企業等に義務付ける暗号化解除法案が出されるなど、様々な議論が巻き起こった。

次に、暗号技術に取り組む企業について紹介する。Apple 社は、暗号機能を強化した新しい OS を発表し、Google 社は、ユーザーに暗号化通信の利用を促す取り組みを進めている。ソーシャルネットワークサービスを提供する企業はエンドツーエンド暗号（通信を行う二者間を結ぶ経路全体の暗号化）を使ったサービスの導入を進めており、非営利組織 Open Whisper Systems が提供しているメッセンジャーアプリ Signal は強力な暗号機能を持ち、大統領候補 Hillary Clinton 氏の選挙キャンペーンで利用されている。また、Facebook 社も同組織のエンドツーエンド暗号機能を自社のサービスに導入している。

最後に暗号技術の研究開発について紹介する。暗号技術では、データベースに多く使われる共通鍵暗号と通信技術に多く使われる公開鍵暗号が主流であるが、近年では、楕円曲線暗号が注目を集めている。連邦政府では、暗号の標準化を進める一方で、ペアリング暗号など次世代の暗号を開発している。暗号解読の手法では、iPhone のロック解除で使われた手法と国際通信網の脆弱性を使った盗聴技術を紹介する。

イギリスは、第二次世界大戦中に電子計算機を使ってドイツの暗号解読に挑んだなど、これまでもコンピューターと暗号技術は競いあってきた歴史があった。現代においても、サイバー攻撃から社会システム、ビジネス、個人情報を守るために強力な暗号が必要となっているが、同時に、多くの人が利用できる形へと変化

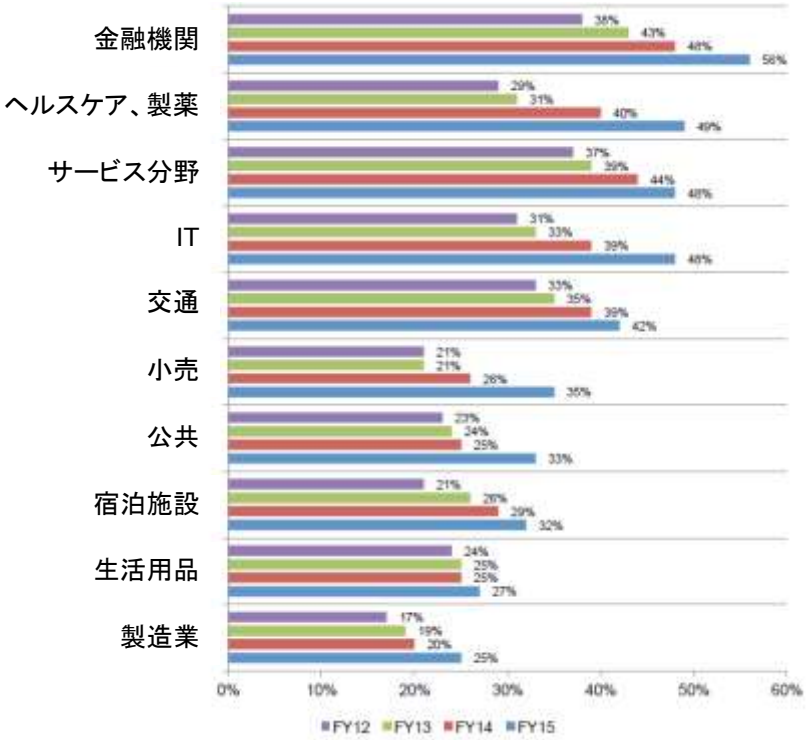
している。一方で、iPhone のロック解除を巡る問題のように、暗号技術が IT の利便性にどのように影響するか様々なバランスも考慮する必要がある。様々な議論を起こしながら IT と暗号技術の進化を進める、米国における暗号技術への取り組みを紹介する。

2 暗号化に関連する市場と動向

(1) 暗号技術の需要と動向

企業が求める IT の暗号技術は、データベースや通信の暗号化に重点が置かれている。情報セキュリティ専門のシンクタンク Ponemon Institute が産業分野の IT 専門家 5,000 人に対して行った調査によると、IT システムの暗号化に包括的な戦略を持っている企業の割合は、2005 年の 15%から 2015 年には 37%へと増加した。各分野別に見た場合、組織全体の IT システムに暗号化を取り入れている企業の割合は、金融や医療などデータの取り扱いに関する法規制がある分野が最も多く、また、全ての産業分野で暗号化に取り組む企業の割合は増加傾向にある。システム別に見た場合、最も多いのがデータベース、インターネット通信、データセンター、イントラネット(VPN[1]を含む)であり、使用頻度の多い IT システムから暗号化への取り組みが進められている。その他、モバイル機器、電子メール、ビジネスソフト、パブリッククラウドでも暗号技術を導入する動きがあり、企業の IT システム全体に対する包括的な暗号化が進められている[2]。
図表 1 は、包括的に暗号技術を導入している企業の割合を分野別に示したグラフとなっている。

図表 1:包括的な暗号技術を導入している企業の割合

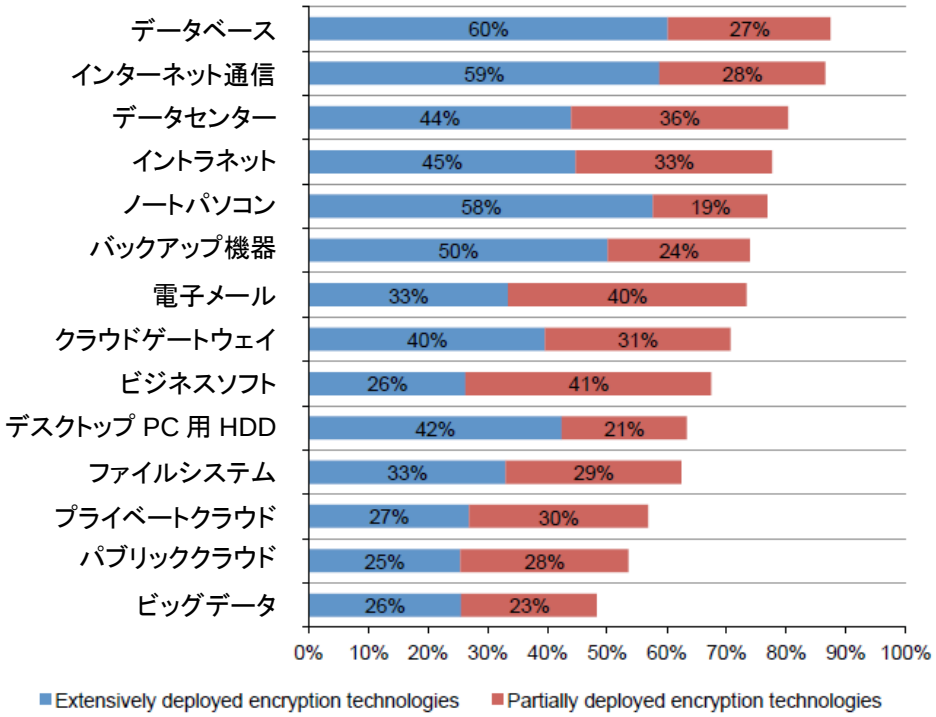


出典:Ponemon Institute[3]

[1] VPN(Virtual Private Network):通信事業者の公衆回線を経由して構築された仮想的な組織内ネットワーク
[2] http://www.ponemon.org/library/2016-global-encryption-trends-study
http://images.go.thales-esecurity.com/Web/ThalesEsecurity/%7B5f704501-1e4f-41a8-91ee-490c2bb492ae%7D_Global_Encryption_Trends_Study_eng_ar.pdf
[3] http://www.ponemon.org/library/2016-global-encryption-trends-study

図表 2 は、企業が暗号化を施しているシステムの割合を示したグラフとなっている。

図表 2:企業が暗号化を施しているシステム



出典:Ponemon Institute[4]

（2） 暗号技術に関連する市場

暗号技術に関連する市場は、ハードウェアとソフトウェアの両方で急速に拡大すると見られている。アイルランドの調査会社 Research and Markets 社は、ハードウェアの暗号技術に関する世界全体での収益は 2015 年から 2020 年にかけて年間成長率 54.6%で急成長すると予測しており、2020 年には 2,964 億ドルに達すると見ている。USB メモリやハードディスクドライブといったデータの保管に関連した製品やネットワーク機器の利用が大きく伸びると見られ、企業や政府機関におけるコンプライアンス向上による需要増加や、価格低下による利用拡大が市場拡大の要因になると見られている[5]。

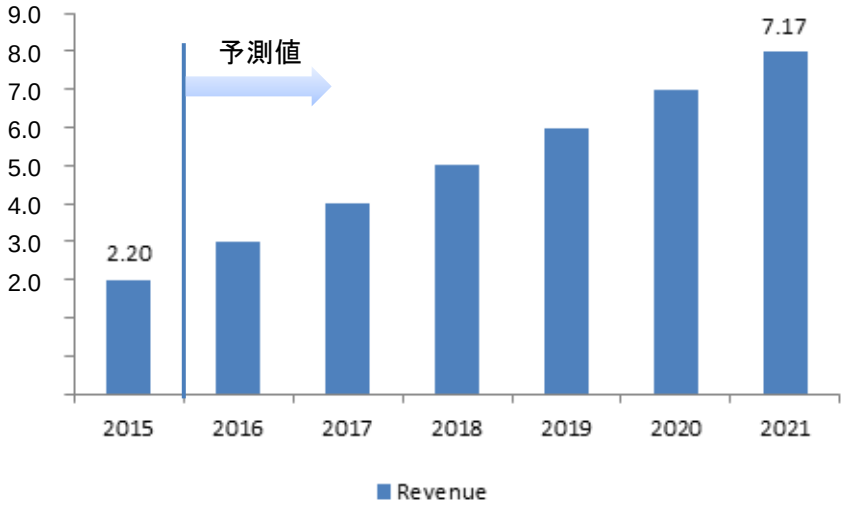
ソフトウェアに関連した暗号技術の市場も急成長が期待されており、米調査会社 Zion Market Research 社は、ソフトウェアを活用した暗号技術の世界全体での収益が 2015 年の 22 億ドルから 2021 年には 71.7 億ドルにまで拡大すると予測している。市場拡大する要因として、情報流出への対策、法規制の拡大、クラウドの利用増加などが大きく、特に、2015 年の市場ではクラウドを対象とした暗号技術が市場の 40%を占めている。現在のところ通信やネットワークよりもデータベース関連の暗号技術の需要が高く、ファイル単位で暗号化を施す File Level Encryption（FLE）とハードディスク全体を暗号化する Full Disk

http://images.go.thales-esecurity.com/Web/ThalesEsecurity/%7B5f704501-1e4f-41a8-91ee-490c2bb492ae%7D_Global_Encryption_Trends_Study_eng_ar.pdf
[4] http://www.ponemon.org/library/2016-global-encryption-trends-study
http://images.go.thales-esecurity.com/Web/ThalesEsecurity/%7B5f704501-1e4f-41a8-91ee-490c2bb492ae%7D_Global_Encryption_Trends_Study_eng_ar.pdf
[5] http://www.researchandmarkets.com/research/mfv98s/world_hardware

Encryption（FDE）の両方が広く使われているが、情報漏えい通知制度などの法規制へ対応するために今後 FDE の利用が増えると見られている[6]。

図表 3 は、ソフトウェアに関連した暗号技術の世界市場となっている。

図表 3：ソフトウェアに関連した暗号技術の世界全体の収益（単位：10 億ドル）



出典：Zion Market Research[7]

3　暗号に関連した事例

（1）　iPhone のロック解除に関する事例

a.　FBI と Apple 社の対立

iPhone のロック解除を巡る FBI と Apple 社の対立は、FBI が外部からの協力を経て解除に成功したことで決着したものの、政府や企業を巻き込んだ大きな議論へと発展した。この問題は、2015 年 12 月にカリフォルニア州 San Bernardino で発生した銃乱射事件において、犯人とテロ組織のつながりが疑われたことから、FBI が犯人の iPhone からデータを取り出すために Apple 社へ技術協力を要請したものの、同社がセキュリティ上の懸念から要請を拒否したというもの。FBI は裁判所へ判断を求め、2016 年 2 月 16 日には、カリフォルニア州の連邦裁判所が FBI に協力する命令を Apple 社へ出したが、同社は、命令の取り消しを申し立てた[8]。また、同社はユーザーに向けて声明を発表し、テロ対策を理由に暗号解除を迫る FBI とユーザーのセキュリティを守るために拒否を貫く Apple 社の対立へと発展した[9]。

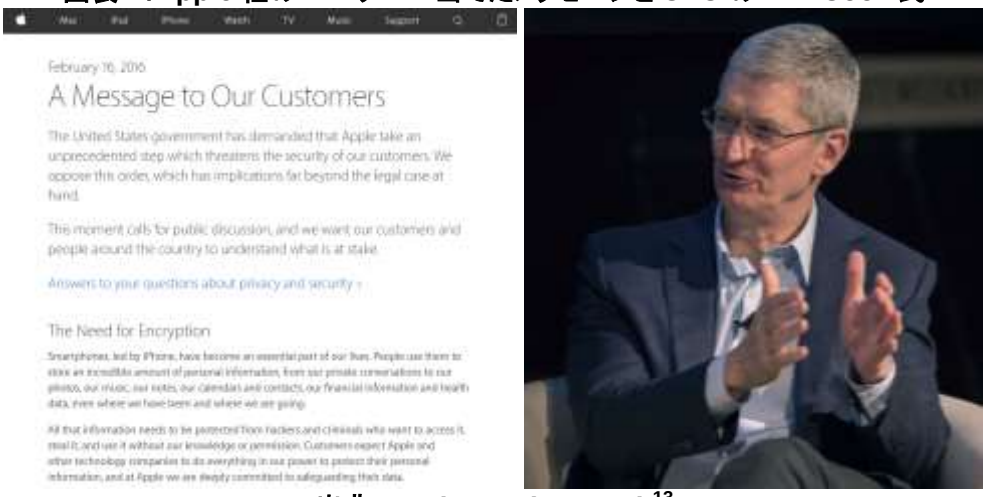
iPhone は、自動消去機能を有効にしている場合には画面ロックのパスコードを 10 回間違えると端末上のデータが消去される仕組みとなっており、端末内のデータは暗号化されているため、暗号化されたデータは FBI だけでなく Apple 社も解読できない。このため、安全にデータを取り出すためにはユーザーがロック画

[6] https://www.zionmarketresearch.com/news/global-encryption-software-market
[7] https://www.zionmarketresearch.com/news/global-encryption-software-market
[8] http://www.wsj.com/articles/apple-files-motion-opposing-order-to-unlock-iphone-1456432357
[9] http://gizmodo.com/why-you-should-care-about-apple-s-fight-with-the-fbi-1759639200
http://www.theverge.com/2016/2/17/11031364/apple-encryption-san-bernardino-response
https://techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-to-unlock-san-bernardino-attackers-iphone/

面で正しいパスコードを打ち込むしか方法がない[10]。連邦裁判所が Apple 社へ出した命令は、自動消去機能を回避するまたは無効にするツールを FBI へ提供するというもので、事件で使われた iPhone だけでなく全機種のセキュリティを回避できる方法であった。このため Apple 社は、セキュリティをすり抜けるバックドア（抜け道）を搭載した iOS[11]を作ることと同じであり、一度作成したツールが他の iPhone へ使用されない保証がない以上、自らの手でユーザーのセキュリティを脅威にさらすことになると反論した[12]。

図表 4 は、Apple 社のユーザーへ当てたメッセージと CEO の Tim Cook 氏となっている。

図表 4：Apple 社のユーザーへ当てたメッセージと CEO の Tim Cook 氏



出典：Apple、Tech Crunch[13]

3 月 1 日に米連邦議会で開かれた公聴会では FBI 長官と Apple 社の代表が主張を繰り広げた[14]。また、ニューヨーク州で起きた覚せい剤事件では司法省（Department of Justice：DOJ）が同様に iPhone のロック解除を求めており、裁判所が Apple 社を支持し DOJ の要請を棄却するなど話が拡大していった[15]。FBI は、Apple 社を命令に従わせるよう裁判所へ要請し、裁判所で新たに審問が開かれる予定であったが、FBI が暗号解読などを得意とする外部からの協力により iPhone のロック解除に成功したため、裁判所への要請を取り下げ、この問題は一応の決着を見せた[16]。しかしながら、ユーザーのセキュリティと捜査への協力というバランスをどのように取るかという議論が、IT 企業、米連邦政府、連邦議会の間で巻き起こった。

b. iPhone の暗号解除を巡る背景

FBI と Apple 社の対立には、プライバシーを重視する IT 企業と情報収集のためにアクセスを求める警察の対立が背景となっている。2013 年 6 月に起こったスノーデン事件によって、通信やデータへのアクセスを政府へ許していた IT 企業は大きな非難を受け、同時に、政府がユーザーのプライバシーを損なうほどの大規模な監視活動を行っていたことから、政府と IT 企業の間の信頼関係は大きく崩れた。このため、一部の IT

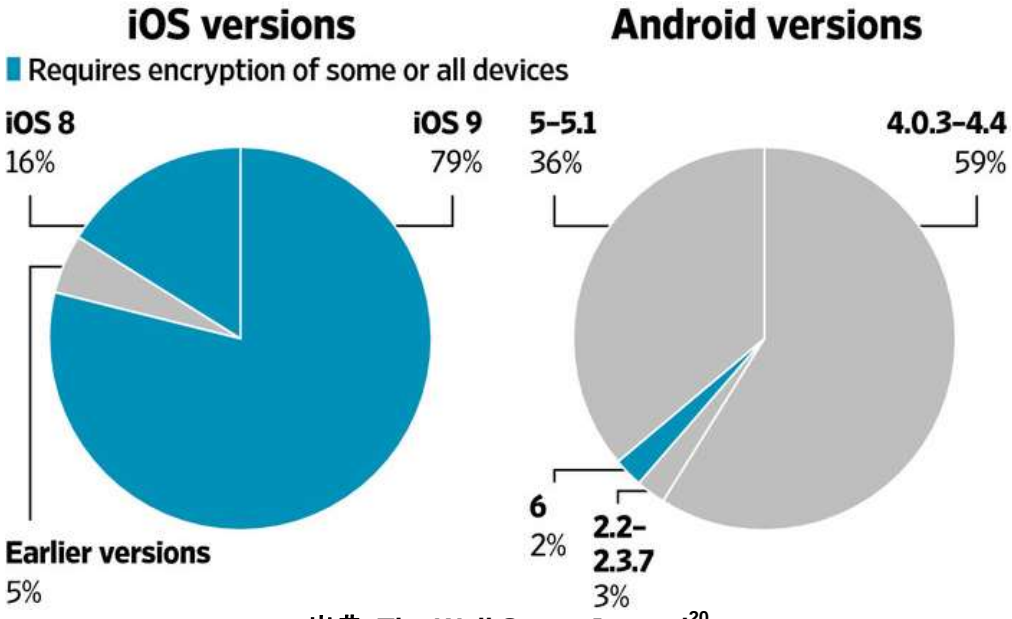
[10] http://www.reuters.com/article/us-apple-court-encryption-idUSKCN0SE2NF20151020
[11] iPhone に使用されているオペレーティングシステム
[12] https://techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-to-unlock-san-bernardino-attackers-iphone/
http://www.apple.com/customer-letter/
[13] https://techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-to-unlock-san-bernardino-attackers-iphone/
http://www.apple.com/customer-letter/
[14] http://gizmodo.com/fbi-director-james-comey-is-a-clown-1762226376
[15] http://gizmodo.com/new-york-judge-rules-us-cant-force-apple-to-help-unlock-1762036873
[16] http://www.zdnet.com/article/justice-dept-files-motion-pushing-apple-to-help-fbi-unlock-iphone/
http://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department-farook/82354040/

企業では、暗号化されたデータへアクセスするための鍵を自ら持たないようにすることでユーザーのみがデータへアクセスできるようにし、企業自身はユーザーのデータの中身を見られないようにしている。Apple 社も、令状があれば法執行機関からの要請に応じて iPhone のロック解除を行ってきたが、2014 年 9 月に発表された iOS 8 以降の端末では、端末全体の暗号化を行うと同時に同社自身が解除のための鍵を保有しなくなったため、同社は近年ロック解除を行っていない。一方で、FBI の James Comey 長官は Apple 社の暗号化を法執行機関に対する攻撃と呼ぶなど強硬な姿勢を見せたことから、FBI と Apple 社は対立へと発展していった[17]。

Apple 社は、同社のクラウドサービス iCloud に残された犯人のデータを提供するなど一定の協力をしており、それにもかかわらず FBI は iPhone のロック解除を Apple 社へ強く迫っている。The Wall Street Journal 紙の調査によると、世界で使われている Android[18]のうち暗号化機能の有効化が必要な機種の割合は 10%以下なのに対し、iOS は 95%に達すると見られ、Apple 社製品の間で暗号化が大きく普及していることが FBI が強硬な姿勢を見せた要因の 1 つとなっている[19]。

図表 5 は、iOS と Android で暗号化されている端末の割合を示した図であり、青色の部分が暗号化されたものとなっている。

図表 5：iOS と Android で暗号化されている端末の割合（2016 年 3 月時点）



出典：The Wall Street Journal[20]

Apple 社は、前 CEO の Steve Jobs 氏がプライバシー保護を重視していたこともあり、セキュリティを高めるために暗号化をいち早く取り入れてきた。2010 年には暗号化通信が可能なビデオ通話機能 FaceTime を発表し、2011 年にはメッセンジャー機能 iMessage を発表している。2007 年に開始された NSA の通信監視プログラム PRISM には Microsoft 社や Google 社などが早い段階で参加したと見られているが[21]、Apple 社は、Steve Jobs 氏が他界した 1 年後の 2012 年 10 月に PRISM へ参加[22]するまで約 5 年に渡っ

[17] http://blogs.wsj.com/digits/2015/12/04/does-encryption-really-help-isis-what-you-need-to-know/
[18] Google 社のスマートフォン用 OS
[19] http://www.wsj.com/articles/google-faces-challenges-in-encrypting-android-phones-1457999906
[20] http://www.wsj.com/articles/google-faces-challenges-in-encrypting-android-phones-1457999906
[21] NSA の文書の中で示されているもので、Microsoft 社と Google 社は PRISM への参加を否定している。
[22] NSA の文書の中で示されているもので、Apple 社は PRISM への参加を否定している。

て協力を拒み続けた[23]。また、現在の CEO Tim Cook 氏も同性愛者であることを公表しており、ユーザーのプライバシー保護を重視している[24]。

Google 社も、自社開発のスマートフォン Nexus には自動で暗号化する機能を搭載し、Android 6.0 から暗号化を要件に入れるなど Android の暗号化へ取り組んできた。しかしながら同社は、自社のサービスにユーザーを呼び込むために Android をスマートフォンメーカーに無償提供しており、暗号化によるパフォーマンス低下を嫌うメーカーからの反発が大きく、メーカーが Android から離れることを恐れて強く主張してこなかった。また、Android は一定の条件下であれば自由に利用できるため、バージョンアップなど最終的な利用方法がメーカーの裁量に委ねられているという背景もあった。対照的に Apple 社は、ハードウェアとソフトウェアの両方を自社で管理しており、必要に応じて iOS の更新を促すことができるため素早く暗号化を普及させている[25][26]。

（2） ロック解除をめぐる論争

iPhone のロック解除を巡る論争は、FBI が外部から得た情報の開示や IT 企業によるセキュリティ強化など様々な方向へと拡大した。FBI は、外部からの協力を得て iPhone のロック解除に成功したが、Apple 社が把握していない脆弱性を利用した方法であったことから、同社が情報の共有を求めていた。連邦政府機関が IT セキュリティの脆弱性を発見した場合には、企業が脆弱性の修正を行うために情報を公開する Vulnerabilities Equities Process（VEP）という規定があり、今回のケースでは、ホワイトハウスの専門家グループが公開の可否を判断する事前審査を行うと見られた。しかしながら FBI は、外部から購入したのはロック解除の方法だけで正式な審査ができるほどの脆弱性に関する技術的情報を持ち合わせていないとして情報を提供しなかった。このため、VEP の審査は実施されず、暗号解除の方法は公にされなかった[27]。

FBI は、外部協力者に iPhone のロック解除に対する報酬として約 100 万ドルを支払ったと見られるが、解除に使われた方法は事件で使われた iPhone 5c にしか有効でないため、上位機種である iPhone 5s やその後に発売された最新機種には利用できないという[28]。上述のニューヨーク州における裁判の中で、国土安全保障省（Department of Homeland Security：DHS）が iPhone の画面ロックを解除せずにデータを抜き出すソフトウェアを所有していることが明らかになっているものの、このソフトウェアも iOS 8.1.2 以降では使えないことがわかっている[29]。

FBI と Apple 社の対立によって論点となったのが法執行機関の捜査に IT 企業がどのように協力するかという問題であった。法執行機関は、IT の暗号化が捜査の障害になりつつあることから IT 企業の協力を必要としているが、一方で、高いセキュリティを目指す IT 企業に対して意図的にセキュリティを落とすことやバックドアの作成を強制することは行き過ぎではないかと IT 企業は大きく反発した。事実、上述のニューヨーク州の覚せい剤事件で使われた iPhone は iOS 7 だったため、司法省（DOJ）と Apple 社の両方がデータを読み取ることができたが、DOJ が要求したのは情報収集のためのロック解除ではなく、ロックを回避する方

[23] https://the01.jp/p0001974/
http://fortune.com/2016/02/21/apple-steve-jobs-privacy/
https://techcrunch.com/2013/06/17/apple-nsa/
http://www.huffingtonpost.com/2013/06/19/apple-nsa-steve-jobs_n_3461323.html
https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[24] http://www.nytimes.com/2016/02/19/technology/how-tim-cook-became-a-bulwark-for-digital-privacy.html
[25] http://www.wsj.com/articles/google-faces-challenges-in-encrypting-android-phones-1457999906
[26] 暗号化機能は Android 4.0 から搭載されているが、ユーザーが自ら暗号化を有効にする必要がある。
[27] http://www.reuters.com/article/us-apple-encryption-whitehouse-idUSKCN0XB05D
http://www.npr.org/sections/alltechconsidered/2016/04/27/475925946/fbi-explains-why-it-wont-disclose-how-it-unlocked-iphone
[28] http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032
http://www.infoworld.com/article/3053476/security/fbi-says-hack-tool-only-works-on-iphone-5c.html
[29] https://techcrunch.com/2016/02/18/no-apple-has-not-unlocked-70-iphones-for-law-enforcement/

法であったため裁判へと発展した[30]。iPhone の暗号解除問題が法廷で争われるようになると多くの IT 企業が Apple 社を支持し、IT 企業や人権団体から 17 件の法廷助言書と 4 件の公開書簡が裁判所へ提出されたという[31]。また、IT 企業の中には Apple 社と同様に暗号化を推し進めることを明らかにした企業が登場しており[32]、例えば、Facebook 社は傘下 WhatsApp 社のサービス全てを暗号化し[33]、Google 社も 2016 年 9 月に発表したビデオ通話アプリ Duo はエンドツーエンド暗号で[34]、新しいパーソナルアシスタント Allo には暗号化通信ができる機能を搭載するなど、大手 IT 企業を中心に暗号化を進める動きが出ている[35]。

（3） 連邦政府と連邦議会の反応

a. 米連邦政府の反応

iPhone のロック解除の問題は連邦政府内でも大きく意見が分かれ、連邦議会では暗号化解除を義務付ける法案まで作られた。連邦政府内では FBI と Apple 社の対立について意見が分かれており、司法省（Department of Justice：DOJ）は暗号化の進歩によって犯罪捜査が難しくなっていると主張しているが、商務省（Department of Commerce：DOC）、国務省（Department of State：DOS）、ホワイトハウスの科学技術政策局（Office of Science and Technology Policy：OSTP）は、機密や情報産業の保護に暗号化は不可欠だと考えている。NSA や国土安全保障省（Department of Homeland Security：DHS）の幹部は、IT 企業との対立により米国製品へ（バックドアが入っているなどの）不信が高まるとテロリストや犯罪者が海外の暗号技術（が使われている製品）を導入する恐れがあるため、Apple 社の対立を反対していたと言われており、省庁間で意見が分かれている[36]。

オバマ大統領は、バックドアを強制するような立法は支持していないものの IT 企業に歩み寄りを求めており、通信事業者や IT 企業に対して暗号化されている通信やデータに捜査官が例外的にアクセスできるよう要請しているという[37]。2016 年 3 月には、個別のケースには言及できないと前置きした上で、暗号化はプライバシーや社会システムを守るために重要だが、問題は犯罪者を捕まえるためにも情報が必要であり、暗号化されたデータへアクセスするための何らかの手段を残しておく妥協が必要であると述べており、妥協点を探る取り組みを進めている[38]。

図表 6 は、暗号化の問題に言及するオバマ大統領となっている。

[30] https://techcrunch.com/2016/02/18/no-apple-has-not-unlocked-70-iphones-for-law-enforcement/
[31] http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html
[32] https://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsapp-plan-increase-encryption-fbi-apple
[33] https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/?mbid=social_fb
[34] http://gizmodo.com/google-duo-is-googles-overdue-crack-at-a-facetime-kille-1777380266
[35] http://gizmodo.com/googles-ai-plans-are-a-privacy-nightmare-1787413031
[36] http://www.reuters.com/article/us-apple-encryption-schism-insight-idUSKCN0W70U5
[37] http://www.reuters.com/article/us-apple-encryption-schism-insight-idUSKCN0W70U5
[38] https://www.bostonglobe.com/news/nation/2016/03/11/transcript-obama-remarks-sxsw/6m8IFsnpJh2k3XWxifHQnJ/story.html

図表 6:暗号化の問題に言及するオバマ大統領

出典:CNN[39]

Apple 社との対立を繰り広げた FBI の James Comey 長官は、2016 年 8 月に開かれたイベントの中で、カリフォルニア州の乱射事件における Apple 社との裁判は必要なものだったが、暗号化の議論を複雑化させてしまったという点で逆効果であったと述べ、暗号化についての議論をさらに進めるために準備を進めていることを明らかにした。FBI は、2015 年 10 月から 2016 年 3 月までに 4,000 台のスマートフォンを押収したが、そのうちの 500 台は暗号化されていたために端末内部へアクセスできなかったという。同長官は、暗号化技術の進歩によって捜査が困難になってきていることから、法執行機関がモバイルデバイスにアクセスするための判断を国民に委ねたいと考えており、大統領選が終わった 2017 年から暗号化と社会の安全について冷静な議論を進めていきたいとの考えを示した[40]。

b. 暗号化解除法案をめぐる動向

連邦議会では、IT 企業に暗号解除を義務付ける法案を提案しようという動きがある。2016 年 4 月、FBI と Apple 社の対立を重く見た米連邦議会上院の有力議員 2 人は、データの暗号化解除を企業へ義務付ける暗号化解除法案を作成した[41]。この法案は、Richard Burr 上院議員(共和党・ノースカロライナ州)と Dianne Feinstein 上院議員(民主党・カリフォルニア州)が中心となってまとめたもので、Compliance with Court Orders Act of 2016(2016 年裁判所命令遵守法)と名づけられ、討議草案として法案提出の前に一般公開された。その内容は、全ての通信事業者と IT 機器を提供する企業に対し、裁判所の命令に応じて情報・データを判読可能(Intelligible)な形で提出する、または、情報・データを取得するための技術支援を義務付けるというもので、判読可能な形について、暗号化されていないまたは復号化(暗号化されたデータの復元)された情報・データと定義されている[42]。Dianne Feinstein 上院議員はウェブサイト上で、個人のデータを守るために強力な暗号は必要だが、テロリストが米国人の殺害を計画しているか知る必要もあると述べている[43]。

図表 7 は、Dianne Feinstein 上院議員と Richard Burr 上院議員となっている。

[39] http://money.cnn.com/2016/03/11/technology/obama-keynote-sxsw-2016/
[40] http://bigstory.ap.org/article/7efad5f542284872b73a0a78ba052824/fbi-chief-calls-national-talk-over-encryption-vs-safety
[41] https://techcrunch.com/2016/04/19/tech-coalitions-pen-open-letter-to-burr-and-feinstein-over-bill-banning-encryption/
[42] http://www.feinstein.senate.gov/public/index.cfm?a=files.serve&File_id=5B990532-CC7F-427F-9942-559E73EB8BFB p.2, 9
[43] http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649

図表 7：Dianne Feinstein 上院議員と Richard Burr 上院議員

出典：Southern California Public Radio[44]

暗号化解除法案に対しては様々な団体から反対の声が上がっている。Google 社、Apple 社、Microsoft 社、Facebook 社などが加盟する IT 分野の 4 業界団体は、両議員宛ての書簡を連名で公開し、政府の命令によってセキュリティが脆弱化する恐れがあり、予期せぬ結果を招く恐れがあると同法案への懸念を示した[45]。オンラインの人権問題に取り組む非営利組織 Electronic Frontier Foundation も同法案への反対を呼びかける特設ページを開き、IT 企業が自らのセキュリティを阻害するよう強いられ、バックドアの作成が多くの人々に影響することになると述べた[46]。オバマ大統領も同法案を支持しない意向であることが報じられ、同法案が提出されれば全力で阻止すると明言する連邦議員も現れるなど、政府・議会内からも反対の声が多く上がった。同法案は今会期中に提出されなかったものの、Richard Burr 上院議員と Dianne Feinstein 上院議員は修正を加えて理解を求めていく考えを示している[47]。

4 暗号技術の活用に取り組む企業

（1） IT 企業の取り組み

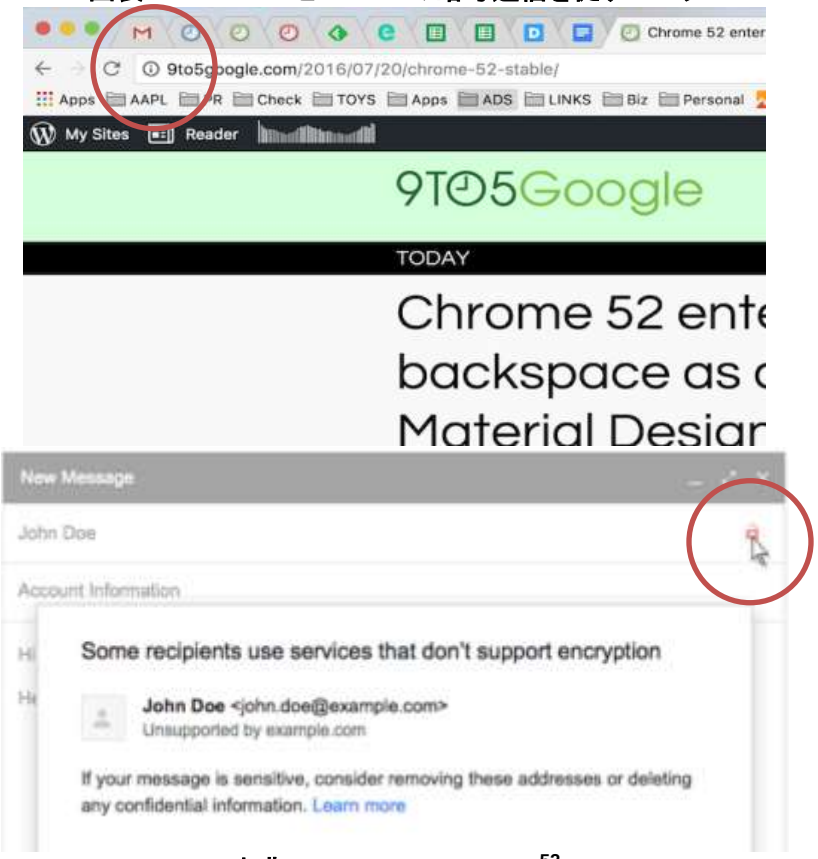
スノーデン事件や iPhone のロック解除を巡るやり取りを経て、IT 企業は、自社のサービスに様々な暗号技術を導入することに乗り出している。Apple 社は、2016 年 6 月に同社の最新 OS である macOS に合わせて暗号化機能を強化した新しいファイルシステム Apple File System（APFS）を発表した。APFS では、①暗号化なし、②単一鍵を使った暗号化、③複数鍵を使った暗号化、の 3 種類の暗号強度を選択することが可能である。同社は、以前から OS に FileVault というディスクボリューム全体を暗号化できる機能を搭載していたが、APFS ではファイル単位での暗号化ができるだけでなく、ファイルのデータとメタデータ[48]が別々に暗号化されるなど、OS レベルで高い暗号機能を提供することが可能となっている。同社は、2017 年から APFS を提供する予定であり、macOS だけでなく、iPhone、Apple Watch、Apple TV、など同社の他の製品にも適用していくことを明らかにしている[49]。

[44] http://www.scpr.org/programs/airtalk/2016/04/14/47986/feinstein-backed-bill-to-mandate-apple-and-others/
[45] http://reformgs.tumblr.com/post/143084034822/letter-to-chairman-burr-and-vice-chairman
[46] https://act.eff.org/action/tell-congress-stop-the-burr-feinstein-backdoor-proposal
[47] http://thehill.com/policy/cybersecurity/295236-report-new-feinstein-burr-encryption-effort-in-works
[48] ファイルの作成日時や形式といった属性情報。
[49] http://arstechnica.com/apple/2016/06/a-zfs-developers-analysis-of-the-good-and-bad-in-apples-new-apfs-file-system/
http://www.techrepublic.com/article/apple-file-system-revealed-at-wwdc-2016-focused-on-encryption-and-ssd-

Google 社は、ユーザーへ暗号化の利用を支援する取り組みを進めており、同社が提供するウェブブラウザ Chrome では、SSL/TLS などで暗号化された通信を行う HTTPS 接続（ウェブサイトの URL が「https:」で始まる）であれば安全であることを示す南京錠のマークが URL の隣に表示され、暗号化されていない通常の HTTP 接続であれば注意を示す「i」のマークが表示される。HTTPS 接続の場合でも「i」マークが表示される場合があり、これは、ウェブサイトへの接続には暗号通信が使われていても、ウェブサイト内で読み込まれる画像などが他のサーバーから HTTP 接続で転送されることを示したものである。Chrome ではウェブサイトの開発者がどこで HTTP 接続になっているか調べるためのツールも用意されている[50]。また、ウェブメール Gmail でもメールの送信先が SSL/TLS 暗号をサポートしていない、または不明な場合には開いた南京錠のマークが表示されるようになっており、メールの送信に暗号通信を利用するように促している[51]。

図表 8 は、Chrome と Gmail の暗号通信を促すマークとなっており、上の画像が Chrome で下の画面が Gmail となっている。

図表 8：Chrome と Gmail の暗号通信を促すマーク



出典：9TO5Mac、Google[52]

support/
[50] https://support.google.com/chrome/answer/95617?hl=en
https://developers.google.com/web/updates/2015/12/security-panel
[51] http://www.zdnet.com/article/gmail-now-alerts-users-to-unsecured-connections/
[52] https://9to5mac.com/2016/07/20/chrome-52-mac-material-design/
https://developers.google.com/web/updates/2015/12/security-panel

（2） エンドツーエンド暗号化の取り組み

ソーシャルネットワークサービス（SNS）を提供する企業を中心に、エンドツーエンド暗号（通信を行う二者間を結ぶ経路全体の暗号化）を使ったサービスの導入が進められている。2013 年に設立された非営利組織 Open Whisper Systems は、エンドツーエンド暗号による通信が可能なメッセンジャーアプリ Signal を提供しており、暗号化されたメッセージ交換や通話が可能である。同アプリでは、画面に表示されるランダムな 2 つの単語を通話の相手に確認することで会話の相手を偽装する中間者攻撃を防ぐことができるようになっており[53]、また、同団体はサーバーに残される利用者の情報が最小限になるように努めている。2016 年前半に、裁判所が利用者の情報提供を同団体に求めた際には、ユーザーのアカウント名、アカウント作成日時、最後に利用した日時の情報しか得られなかったという[54]。この他、大統領候補 Hillary Clinton 氏の大統領選挙キャンペーンにおいても、Signal が利用されるなど注目を集めており[55]、Signal に使われている通信プロトコルは Signal Protocol としてオープンソースで提供されている。

Facebook 社傘下の WhatsApp 社は、2016 年 4 月、同社のサービス全てをエンドツーエンド暗号化したと発表した。同社は 2014 年から Signal Protocol の導入を進め、iPhone や Android だけでなく Windows Phone や Blackberry など展開している全てのプラットフォームで暗号化に対応したという[56]。2016 年 10 月には、Facebook 社がメッセンジャーアプリ Facebook Messenger に Signal Protocol を使ったエンドツーエンド暗号化機能 Secret Conversations を発表した。ユーザーが Secret Conversations を有効にすると会話に参加しているユーザーのメッセージが暗号化される仕組みで、端末間で暗号化が施されるため、Facebook 社でもメッセージの内容を見ることができない。また、一定時間でメッセージを消去する自動消去機能も搭載しており、タイマーを設定すればメッセージが会話から消去される。現在のところ、Secret Conversations を利用できるのは iOS と Android の Facebook Messenger アプリに限られており、Facebook のチャット機能や会話に利用した端末以外ではメッセージを見ることができない[57]。

図表 9 の左の画像は WhatsApp 社の暗号化の概要となっており、右の画像は Facebook Messenger の Secret Conversations 機能となっている。

図表 9：WhatsApp の暗号化の概要（左）と Facebook Messenger の Secret Conversations（右）

出典：Wired、PCWorld[58]

[53] https://www.wired.com/2014/07/free-encrypted-calling-finally-comes-to-the-iphone/
[54] http://www.theregister.co.uk/2016/10/04/whisper_systems_signal_subpoena/
[55] http://fortune.com/2016/08/29/clinton-campaign-signal/
[56] https://techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout/
[57] http://www.wired.co.uk/article/messenger-secret-messages-end-to-end-encryption
[58] https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/
http://www.pcworld.com/article/3128107/security/how-to-encrypt-your-facebook-messages-with-secret-

（3） 金融分野における暗号技術の活用

金融分野における暗号技術には、通信やデータベースの暗号化に加えて、ブロックチェーンが注目を集めている。ネットワークソリューションを提供する Ciena 社は、2016 年 1 月、光ファイバー内の通信を暗号化するソリューション WaveLogic Encryption を発表した。この技術は、光ファイバーを使って送られるデータを暗号化するというもので、高速で暗号化することにより低遅延で最大 200 Gbps でのデータ転送が可能である[59]。韓国の銀行が同社のソリューションを導入する予定であり、プライベートクラウドとデータセンターの間を結ぶ光ファイバー回線の暗号化に使われるという[60]。米ベンチャー企業 ZeroDB 社は、金融機関向けにビッグデータやクラウドのための暗号化サービスを提供している。金融機関は、ビッグデータやクラウドの有用性を理解しながらもコストや処理能力の問題からクラウドの活用を断念しているが、同社のサービスでは、独自のアルゴリズムを使って高速で暗号化を行い、エンドツーエンド暗号により安全にクラウドへ接続できる仕組みとなっており、また、暗号化されたままの状態でデータベースの検索、並び替え、操作、共有ができるという。現在、イギリスの銀行とパートナーシップの締結を進めている[61]。

新しい通貨の可能性として注目を集めているブロックチェーンは、ベンチャー企業と大手金融機関が提携して新しい通貨としてのシステム構築を進めている。米ベンチャー企業 R3 社は、70 の金融機関とともに新しいブロックチェーンのプラットフォーム Concord の構築を進めている。Concord では、銀行内とブロックチェーンの市場を結ぶ共通プラットフォームであり、取引決済、資産登録、勘定調査、現金残高など銀行の後方業務まで含めたものとなっている。R3 社は、Concord の特許を申請しており[62]、2016 年 9 月には参加金融機関との間で同プラットフォームを使ったブロックチェーンのテスト運用が行われた[63]。

5 暗号技術の研究

（1） 暗号技術の研究

a. 様々な種類の暗号

様々な種類の暗号技術が開発され利用が進められているが、より強力な暗号が求められるようになっている。暗号化の方式には様々な種類があるが、大きく分けて共通鍵暗号と公開鍵暗号の 2 つがあり、共通鍵暗号は暗号化と復号化で同じ鍵を使用するが、公開鍵暗号では暗号化（公開鍵）と復号化（秘密鍵）に異なる鍵を使用するという違いがある。共通鍵暗号は、処理が早いため機密性の高いデータの保管（Data at rest）の暗号化に多く使われ、公開鍵暗号は、処理が遅いものの鍵の管理が容易であるためインターネットの暗号通信などデータの移動（Data in motion）に多く利用される。インターネットショッピングなどで個人情報を送信する際に使われる SSL/TLS 通信は、共通鍵暗号と公開鍵暗号を併用したものである[64]。

conversations.html
[59] http://www.lightwaveonline.com/articles/2016/01/ciena-wavelogic-encryption-offers-optical-layer-encryption-up-to-200-gbps.html
[60] https://datacenternews.asia/story/ciena-encryption-boosts-data-center-security-biggest-korean-financial-co/
[61] http://news.softpedia.com/news/zerodb-end-to-end-encryption-database-engine-goes-open-source-497420.shtml
http://motherboard.vice.com/read/the-zerodb-database-offers-end-to-end-encryption-and-even-useful-data-operations
http://sociable.co/data/exclusive-zerodb-cofounder-maclane-wilkison/
https://techcrunch.com/2016/08/22/y-combinator-demo-day-summer-2016/
[62] http://www.wsj.com/articles/bitcoin-tech-firm-thinks-this-name-can-unify-wall-street-behind-blockchain-1472044968
[63] http://www.coindesk.com/r3-banks-startups-test-blockchain-system-syndicated-loans/
[64] https://www.ciphercloud.com/blog/cloud-information-protection-symmetric-vs-asymmetric-encryption/
https://www.virtru.com/blog/enterprise-encryption-solutions/

インターネットの普及により公開鍵暗号が大きく使われるようになり、新しい公開鍵暗号の研究が進められている。公開鍵暗号は、計算結果から元の情報を逆算することが困難な一方向関数という性質を利用することで、暗号化するための公開鍵を公開しても、暗号化されたデータを逆算できないようにしており、現在普及している RSA 暗号は、桁数の大きい素数を用いた素因数分解が非常に困難であるという性質を利用している[65]。RSA に続く暗号として注目を集めている楕円曲線暗号は、楕円曲線論における逆の計算が難しい性質を利用しており、鍵(鍵長[66])が短いため RSA よりも処理が早いという利点がある[67]。

b. 連邦政府の取り組み

米連邦政府は、NIST が中心となって暗号技術の標準化と研究開発が進められている。米国では、暗号を軍事技術と位置づけていたため厳しい輸出規制を敷いていたが、インターネットとの発達とともに電子商取引のための暗号技術が必要となり、1996 年にクリントン大統領が出した大統領令により規制が緩和された。現在では、国家安全保障局(National Security Agency:NSA)と NIST を中心に、政府向けに暗号技術の策定や研究開発が進められている[68]。NIST は、ハードウェアやソフトウェアに使われる暗号モジュールのセキュリティ要求事項として FIPS 140-2[69]を提供しており、連邦政府への調達で要件とされている暗号モジュールの評価試験 Cryptographic Module Validation Program に使われている[70]。最新版である FIPS 140-3 の策定が進められているが、国際標準規格のセキュリティ要求事項である ISO/IEC 19790:2012 の採用も検討されている[71]。現在、NIST が政府機関における調達で利用可能としている暗号には以下のようなものがある。

図表 10 は、NIST が推奨する暗号方式となっている。

図表 10:NIST が推奨する暗号方式

分類	暗号の種類	2030 年まで	2031 年以降
暗号化・復号化	2 Key トリプル DES	暗号化は使用禁止、復号化はレガシーユース(暗号済みの情報に対してのみ使用可能)	
	3 Key トリプル DES	利用可能	暗号化は使用禁止 復号化はレガシーユース
	AES	利用可能	
ハッシュ関数	SHA-1	暗号化は使用禁止、復号化はレガシーユース	
	SHA-2(SHA-224、SHA-512/224)	利用可能	暗号化は使用禁止 復号化はレガシーユース
	SHA-2(SHA-256、SHA-512/256、SHA-384、SHA-512)	利用可能	
	SH-3(SHA-224)	利用可能	暗号化は使用禁止 復号化はレガシーユース
	SH-3(SHA3-256、SHA3-384、SHA3-512)	利用可能	

[65] http://searchsecurity.techtarget.com/definition/RSA
[66] 暗号の鍵となるデータの量のことで、bit(ビット)で表される。鍵長が大きいと CPU の処理増大や、サーバーの通信接続数減少につながる。
https://blog.digicert.com/moving-beyond-1024-bit-encryption/
[67] https://www.globalsign.com/en/blog/elliptic-curve-cryptography/
[68] http://www1.american.edu/TED/cryptog.htm
http://www.ipa.go.jp/files/000046418.pdf
[69] Federal Information Processing Standard(連邦情報処理基準)の略で、情報処理に関する標準規格を定めている。FIPS 140-2 では暗号モジュールの標準規格が規定されている。
[70] http://csrc.nist.gov/groups/STM/cmvp/standards.html
[71] http://csrc.nist.gov/groups/ST/FIPS140_3/
http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/fips-140_response.pdf

電子署名	RSA/DSA（1024 bit）	使用禁止	
	RSA/DSA（2048 bit）	利用可能	暗号化は使用禁止 復号化はレガシーユース
	RSA/DSA（3072 bit 以上）	利用可能	
	ECDSA（160～223 bit）	使用禁止	
	ECDSA（224～255 bit）	利用可能	暗号化は使用禁止 復号化はレガシーユース
	ECDSA（256 bit 以上）	利用可能	

出典：NIST[72]

c. NIST の暗号技術の開発

暗号技術の研究開発では、多様な IT に対応するための次世代暗号の研究が進められている。NSA と NIST では、IoT 向けに限られたデータ量で十分な耐性を持つ軽量暗号（Lightweight Cryptography）の研究開発を進めている。現在、標準規格として定められている暗号の多くが通常のコンピューターを想定したものであり、IoT で使われる小型デバイスではメモリや処理能力が限られるため同じ暗号を使うことが難しく、IC チップ（RFID）を使う場合には保存できるデータ量が少ないなど様々な制約があり、また、コネクテッドカーの場合には低遅延など高い要求が求められるなど、IoT には少ないデータ量で暗号化が可能な軽量暗号が不可欠となってきている。NSA が 2013 年 6 月に発表した SIMON と SPECK は IC チップでの利用を想定した軽量暗号であり、暗号に使用する回路の数が従来の 6 割ほどしか必要としない軽量設計であるため、小型デバイスの利用に適している。SIMON がハードウェア側で、SPECK がソフトウェア側での利用を想定しており、この 2 つは現在、軽量暗号の国際標準規格 ISO/IEC 29192-2 へ標準規格に提案されている[73]。NIST も 2013 年から軽量暗号の研究を進めており、2016 年 8 月には軽量暗号の標準化策定の計画案 NISTIR 8114 を発表し、2016 年 10 月には 2 日間にわたるワークショップを開催するなど、軽量暗号の確立に向けた取り組みを進めている[74]。

この他、NIST や国防高等研究計画局（Defense Advanced Research Projects Agency：DARPA）では、以下のような暗号に関連した研究が進められている。

＜ペアリング暗号（Pairing-Based Cryptography）＞

楕円曲線暗号を発展させた公開鍵型の暗号で、自由なキーワードを使って公開鍵を作成できるという特徴を持っているため、以下のような応用が可能と見られている[75]。

- ID ベース暗号：メールアドレス、氏名、携帯電話番号といった、個人を識別できる情報を鍵にして暗号化する方法。データを暗号化して送信する側は、受け取り側の個人識別ができる情報を鍵にして送るため先に公開鍵を受け取る手順を踏む必要がない[76]。
- 時限式暗号：タイムスタンプを鍵にすることで、指定した時間にのみデータを復号できる暗号。
- 検索可能暗号：データベースを暗号化したままで、データの内容を検索できる暗号。クラウドへの応用が期待されている。

＜プライバシー保護暗号（Privacy Enhancing Cryptography）＞

[72] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf p.4, 6, 7, 14
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf p.53, 54, 56
[73] http://www.rfidjournal.com/articles/view?13288/
[74] https://www.nist.gov/news-events/events/2016/10/lightweight-cryptography-workshop-2016
[75] http://csrc.nist.gov/groups/ST/crypto-research-projects/#PBC
http://www.atmarkit.co.jp/ait/articles/1508/25/news003.html
[76] 実際には、信頼できる第三者機関が誰にでも利用可能な公開鍵を先に配布し、送り側は、受け取り側の個人識別できる情報で暗号化する。その後、受け取り側は第三者機関に本人確認をしたのちに復号するための秘密鍵を入手する。

ゼロ知識証明（Zero-knowledge proof）という方法を使うことで、暗号を解除せずに（データの内容を覗かず）データが編集されたかどうかを確認できる。以下のような応用が可能になると見られている[77]。

- ブラインド署名：データを復号させずに署名を入れることができる。電子署名や電子投票に活用できる。
- グループ署名：暗号化されたままで、個人は特定せずに署名している人が所属しているグループや部署名などを確認する。会員サービスなどで、サービス提供者へ個人情報を渡さずに会員であることを証明できる。
- データの検証：データを暗号化したままで、データの内容を検証する。例えば、オークションの入札において、複数の入札データの中で最も大きな入札額だけを確認するといった使い方ができる。

＜乱数ビーコン（Randomness Beacon）＞

60 秒ごとに 512bit の完全な乱数をインターネット上で配信する取り組み。過去の乱数は配信した時間と一緒にウェブサイト上で確認できるため、電子署名の作成日時の証明などに利用できる[78]。また、プライバシー保護暗号と組み合わせることで、指定時間になると一番高い入札者のデータだけ復号されるという使い方もできる[79]。

＜耐量子暗号（Post-Quantum Cryptography）＞

現在の暗号技術を容易に破ることが可能な量子コンピューターが 2030 年には登場すると見られており、量子コンピューターに対抗できる耐量子暗号の開発が進められている[80]。2017 年後半までにアルゴリズムの公募を行い、3～5 年かけて標準化に向けた調査を行う[81]。

＜PROgramming Computation on EncryptEd Data（PROCEED）＞

クラウド上のデータを暗号化させたまま書き換える方法を研究する国防高等研究計画局（DARPA）のプログラムで、完全準同型暗号（Fully homomorphic encryption）という方法が検討されている[82]。

（2） 様々な暗号解読の手法

a. iPhone のロック解除の試み

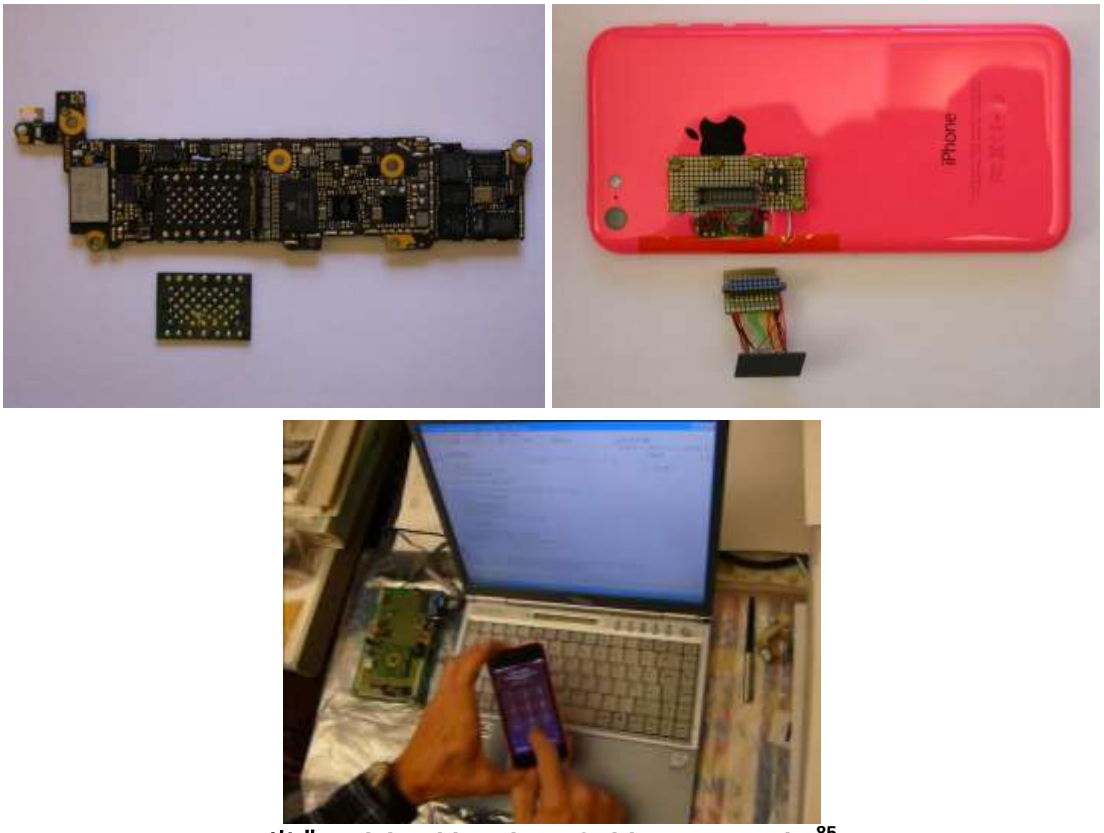
新しい暗号の登場とともに暗号解読の手法も多様化しており、近年では、脆弱性を突いて暗号を回避する手法が多く使われている。Apple 社に iPhone のロック解除を迫った FBI は、最終的に外部ハッカーの支援を受けてデータの取り出しに成功したが、その詳細は明らかにしていない。Washington Post 紙は、Apple 社が把握していないソフトウェアの脆弱性を利用したと見られているが、iPhone の自動消去機能を無効化してパスコードを割り出す方法を使用したとも報じている[83]。最も有効とされる iPhone の自動消去機能を無効化する方法の 1 つに NAND ミラーリングがある。これは、端末内部でデータを保存している NAND メモリの内容を外部にコピーして保存し、パスコードを制限回数まで入力して iPhone が自動消去されると、保存した内容を復元して、消去される前に戻してしまうというもの。これによりパスコードを無制限に試すことができるため、自動消去機能を事実上無効化できる。英国ケンブリッジ大学の Sergei Skorobogatov 教授が NAND ミラーリングを試みたところ、実際にパスコードの割り出しに成功しており、4 桁のパスコードであれば 24 時間もかからずに全て試すことができるという。FBI の James Comey 長官は、NAND ミラーリングで

[77] http://csrc.nist.gov/groups/ST/crypto-research-projects/#PEC
http://www.atmarkit.co.jp/ait/articles/1510/20/news007.html
[78] https://www.nist.gov/programs-projects/nist-randomness-beacon
[79] http://csrc.nist.gov/groups/ST/crypto-research-projects/#PBC
[80] http://japan.zdnet.com/article/35087380/
http://www.zdnet.com/article/encryptions-quantum-leap-the-race-to-stop-the-hackers-of-tomorrow/
[81] http://csrc.nist.gov/groups/ST/post-quantum-crypto/
[82] http://www.darpa.mil/program/programming-computation-on-encrypted-data
[83] https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html

はうまくいかないと発言しており、専門家は、この方法では端末内部を壊す可能性があるため FBI にとって実用的でないのかもしれないと述べている[84]。

図表 11 は、実際に NAND ミラーリングにより iPhone の自動消去機能を回避する実験の様子となっており、上の画像は NAND メモリを基盤から取り外して、付け外ししやすくした状態となっており、下の画像は実際にパスコードを打ち込んでいる様子となっている。

図表 11：NAND ミラーリングを使った実験



出典：Zdziarski's Blog of Things、Youtube[85]

b. 国際通信網の盗聴

国際通信網の脆弱性を使い、電話番号だけで世界中のどこからでも携帯電話を盗聴できる方法が明らかになっている。この方法は、国際通信網に使われている通信プロトコル Signaling System No. 7（SS7）の脆弱性を使い、携帯電話の通話内容、テキストメッセージ、位置情報を取得できるというもので、世界中のどこにいても電話番号だけでターゲットとする携帯電話を盗聴できるという。ドイツのセキュリティ企業 Sternraute 社の Tobias Engel 氏と Security Research Labs 社の Karsten Nohl 氏が発見したもので、2014 年 12 月のハッカーカンファレンスで研究内容を発表した。発表された内容では、電話の転送機能を乗っ取り、通話を転送させて盗聴するという方法と、街中で発信されている 3G 回線の電波を自作の電波塔で読み取るという方法が紹介された。3G 回線の電波は暗号化されているものの、SS7 経由で携帯電話キャリアにリクエストを送れば復号のための鍵を送ってくれるという[86]。

[84] https://www.wired.com/2016/09/heres-fbi-hacked-san-bernardino-shooters-iphone/
[85] https://www.zdziarski.com/blog/?p=6015
https://arxiv.org/ftp/arxiv/papers/1609/1609.04327.pdf
https://www.youtube.com/watch?v=tM66GWrwbsY
[86] https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-

2016 年 4 月、米国のドキュメンタリー番組 60 Minutes で行われた実験では、実験に協力した Ted Lieu 下院議員（民主党、ニューヨーク州選出）が使用している iPhone の通話やテキストメッセージを盗聴し、どこにいるかリアルタイムで位置を把握した。また、電話をかけてきた発信元の電話番号を知ることも可能であり、Ted Lieu 下院議員は、オバマ大統領が電話してきたことがあるが、大統領の電話番号やその通話内容をハッカーが把握できるとすれば恐ろしいと述べた。人権団体 American Civil Liberties Union（ACLU）は、ほとんどの諜報機関が SS7 の研究チームを所有しており、諜報活動に SS7 の脆弱性を利用しているのではないかと述べた。SS7 の盗聴を防ぐためには、iMessage、WhatsApp、Signal といったエンドツーエンド暗号を使ったアプリのメッセージ機能や VoIP 機能が有効と見られている[87]。

6 終わりに

ハッキング、情報漏えい等が大きな社会問題になっている中、サイバーセキュリティは益々重要な課題となっており、その対策の一つである暗号化技術は、今やなくてはならない存在と言える。さらに、これから本格的な IoT の時代を迎えるにあたり、ますますセキュリティ対策が重要になり、強力な暗号が必要となる一方で、少ないデータ量で暗号化を可能とするより軽量な暗号化技術が必要とされるなど、暗号化の更なる技術発展が期待されている。
しかし強力な暗号化は、場合によっては利便性を損ねる恐れがあるだけでなく、米国でおきた iPhone のロック解除に関する FBI と Apple 社の法廷闘争のように、暗号化に関する新たな課題も起きている。IT 化が進めば進むほど重要性が増す暗号化の技術発展と、それをとりまく様々な課題については、今後も注視していくことが必要であろう。

let-anyone-listen-to-your-cell-calls-and-read-your-texts/
[87] https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/
http://www.cbsnews.com/news/60-minutes-hacking-your-phone/
https://9to5mac.com/2016/04/18/ss7-hack-iphone-congressman/
https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls