2016年6月16日
デジタル・フォレンジック研究会「法務・監査」分科会

iPhoneロック解除問題とデジタル・フォレンジック

湯淺　墾道
情報セキュリティ大学院大学　教授

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

自己紹介

- 青山学院大学法学部公法学科卒業、同大学院法学研究科公法専攻博士前期課程修了、慶應義塾大学大学院法学研究科政治学専攻博士課程退学
- 慶應義塾大学講師等をへて、2004年九州国際大学法学部専任講師、2005年助教授、2007年准教授、2008年教授・副学長、2011年情報セキュリティ大学院大学情報セキュリティ研究科教授、2012年学長補佐
- 総務省ICTインテリジェント化影響評価検討会議構成員、神奈川県情報公開・個人情報保護審議会委員、埼玉県本人確認情報保護審議会会長、埼玉県特定個人情報保護委員会委員長、北九州市男女共同参画審議会副会長、川崎市情報公開運営審議会副会長、渋谷区情報公開及び個人情報の保護審議会委員、一般財団法人日本データ通信協会電気通信個人情報保護推進センター諮問委員長、ベネッセホールディングス情報セキュリティ監視委員会委員長代理　ほか
- 東京中小企業サイバーセキュリティ支援ネットワーク(Tcyss)有識者委員
- http://home.att.ne.jp/omega/yuasa/index.html

ロック機能や暗号化の背景

通信傍受を認める法制度

- 総合犯罪防止安全市街地法(Omnibus Crime Control and Safe Streets Act of 1968)
- 外国情報活動監視法(Foreign Intelligence Surveillance Act of 1978)
- 通信傍受法(Communications Assistance for Law Enforcement Act of 1994)
- 愛国者法(Patriot Act of 2001)
  - 外国情報活動監視裁判所(United States Foreign Intelligence Surveillance Court)

FISA Courtの令状発給

■ **2004年から2012年までの間に15100件の傍受許可令状を発給し、令状発給を退けたのはわずか7件**

■ **2014年1月**

- **Facebook、Google、LinkedIn、Microsoft、Yahoo等の企業が外国情報活動監視裁判所によって情報提供を求められている件数を公開することを許可**
- それ以外の情報の公開は不許可
  - ◆Evan Perez, *Secret Court's Oversight Gets Scrutiny*, WALL STREET JOURNAL, June 9, 2013, http://www.wsj.com/articles/SB10001424127887324904004578535670310514616.

暗号化の現状

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■「無法地帯」か「専制からの解放」か

- 通信傍受法
  - ◆端末からメッセージが送信されたり、外部のサーバーに保存されたりした後の通信内容に対して捜査機関がアクセスすることを支援するように通信事業者等に対して求める
  - ◆ユーザー個人のスマートフォン等の端末自体は法の射程に入っていない
- FBIと司法省は、通信傍受法がインターネットを利用したメッセージ交換、SNS、P2P等のサービスに対しては有効に機能していないと主張

事案の概要

iPhone事案の概要

	カリフォルニア事案	ニューヨーク事案
発生時期	2015年12月発生	2014年6月逮捕
iPhoneの所有者	被疑者が 勤務していた郡	被疑者
被疑者	警察の銃撃戦で死亡	生存
事案・被害者	銃の乱射・14人が死亡、 22人が負傷	麻薬密売等
裁判所	カリフォルニア 中央地区連邦地裁	ニューヨーク東部地区 連邦地裁
地裁の判断	捜査機関のiPhoneの データへのアクセス 支援を命令	全令状法に基づく Apple社への命令の 求めを退ける

カリフォルニア州の事件

■2015年12月にカリフォルニア州で14人が死亡、22人が負傷した銃の乱射事件が発生

- ●令状により被疑者のiPhoneを押収
- ●被疑者は警察の銃撃で死亡
- ●被疑者使用のiPhoneの所有者は、被疑者の勤務先の郡政府、解析に同意
- ●ロック機能のため解析できず
- ●Appleに対して支援を要請したが、Appleは拒否

ニューヨーク州の事件

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■2015年、麻薬捜査局がニューヨークで麻薬取引捜査

- ●被疑者のiPhoneを令状により押収
- ●iPhoneの所有者は被疑者
- ●2週間という令状の期限内ではロック機能を解除することができず、FBIに支援を求めた
- ●FBIも解除に成功せず、令状の期限が過ぎた後にApple社に支援を求めた
- ●Appleは支援を拒否

治安判事の判断 カリフォルニア

- 2016年2月16日に3頁の書面で決定
- Apple社に対して、捜査機関がiPhoneのデータにアクセスできるように支援することを命令
  - iPhoneの自動消去機能の回避または停止
  - パスコードの提供、FBIが提供されたパスコードでiPhoneにアクセスした際に他のデータを削除しないようにすること
  - また可能であれば、パスコードを10回間違ってもデータが消去されないようにするツールも提供する
  - 他の技術的な方法でこれらに代わる措置を提供できるのであれば、FBI側と協議した上で、それに代えることもできる
- 特に命令自体の適法性には触れず

治安判事の判断 ニューヨーク

- 50頁にものぼる書面で決定
- 全令状法に基づくApple社への命令を否定
  - そもそも裁判所は全令状法に基づきロック機能解除命令を出すことができるか、という点を問題視
  - 政府側が全令状法に基づいて裁判所がApple社に命令を出すことができる根拠を十分に証明していない
  - 仮に出すことができるとしても、今回の事情を考慮すると、Apple社に命令を出すに足る要素は存在しない
    - ◆全令状法による令状を第三者に出すことができるのは、やむを得ない場合に限られる
    - ◆本件の事情を検討すると、やむを得ない場合に当たらない

■やむを得ない場合に該当するかを
判断する際に考慮すべき点
- ●被疑者の犯罪及びその捜査とApple社との関係
- ●Apple社に課すことになる負担の大きさ
- ●Apple社にそのような負担を課さなければならない必然性

■本件では、いずれもApple社に政府を支援する義務を課すことを正当化するものではない

その後

■カリフォルニア州事件
- ●FBIが取り下げ(3月28日)
  - ◆The government has now successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple Inc. mandated by Court's Order Compelling Apple Inc. to Assist Agents in Search dated February 16, 2016.

■ニューヨーク州事件

●FBIが取り下げ（4月22日）

◆「ある個人(an individual)から
パスコードを入手したので、
Appleの支援が不要になった」

◆被疑者本人から入手したのか
どうか等、詳細は不明

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

全令状法に関する検討

全令状法(All Writs Act)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 28 U.S.C. § 1651.
  - もともとは1789年に制定された司法部法(Judicially Act)の一部
  - 1911年に現在の形
- 条文
  - (a)連邦最高裁判所と連邦議会によって設立された全裁判所は、その権限を行使する上で必要もしくは適切であり、かつ法の慣習及び原理の上で許される全令状を発給することができる。
  - (b)代替令状もしくは仮命令は、管轄権を有する最高裁判所裁判官もしくは(下級裁判所の)裁判官によって発給することができる。

連邦最高裁の解釈

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- プライス対ジョンストン判決(1948年)
  - 全令状法は、「法の合理的な終結(the rational ends of law)」を達成するために連邦議会によって認められた手続的な手段
- 適用を制限
  - 他の法律上の手段がない場合
  - 連邦裁判所自身が管轄権を持っている場合
  - 連邦裁判所の権限を行使する上で必要または適切である場合
  - 令状の内容が議会によって制定された法律に反しない場合

合衆国対電話会社判決（1977年）

- ニューヨーク市内で違法賭博を行っている可能性のある企業が捜査の対象
- FBIは、電話会社に対して当該企業が使用していた2台の電話機からダイヤルを回した先を記録する装置(pen register)取り付けを要請
- 電話会社は拒否
- FBIは、全令状法に基づき記録装置を取り付け情報提供すると共にFBI捜査官を支援する命令を発出することをニューヨーク州南部地区連邦地裁に求めた
- 1976年3月19日、連邦地裁はFBIの主張を認めて、電話会社に対し記録装置を取り付ける命令を発出

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■争点

- ●連邦裁判所は、全令状法により、被疑者や被疑者と直接の関係がある者だけではなく、被疑者と直接関係のない者（第三者）に対しても命令を下すことができるのか
- ●第三者にとって過重な負担にならないか

■ 第2巡回区連邦控訴裁判所

- ●連邦裁判所が被疑者と直接関係のない第三者に対して命令を下すことはできないとして、電話会社の異議を認めた
  - ◆電話会社が支援を拒否した理由
    - ➢電話会社が支援することによって、政府がネットワークにアクセスした場合、政府による「無差別的プライバシー侵害」を帰結することになる
- ●電話会社の主張を認める

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 連邦最高裁

- ●「エドワード1世の時代から、市民を国家の司法を執行するために招集することは許される」(引用)
- ●「私人である市民は、要請を受けたときには法執行機関に対して**援助を提供する義務**を有する」
- ●「全令状法に基づいて連邦裁判所が**第三者**に対して無制限に命令を出すことができるというわけではなく、**不合理な負担を課す**ことは許されない。しかし、本件における命令の内容は、全令状法によって明確に授権されたものであり、連邦議会の立法趣旨にも合致するものである」

ニューヨーク事案

■ ニューヨーク東部地区連邦地裁のオーレンスタイン連邦治安判事が、50頁にものぼる書面で決定を下し、全令状法に基づくApple社への命令を否定

- ●そもそも裁判所は全令状法に基づきロック機能解除命令を出すことができるか
  - ◆全令状法による令状を出すことができるのは、やむを得ない場合に限られる
  - ◆被疑者のフェンの犯罪及びその捜査とApple社との関係、Apple社に課すことになる負担の大きさ、Apple社にそのような負担を課さなければならない必然性という3点を考慮

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

1. 電話会社は規制を受ける公益事業であるから負担を課すことも許容されるが、私企業にすぎないApple社（と、結果的にその株主）に他の企業よりも重い義務を課すことの必然性を政府は立証していない。
2. Apple社は顧客の個人的なデータをいかなる不正アクセスからも守るリーダーシップの役割を果たすことで競争的市場における成功をおさめてきたのであり、明確な法的根拠なしにApple社がロック解除の支援を行うことはApple社と顧客との間の信頼関係にひび割れを生じさせる。
3. ダイヤル先記録装置の装着が問題となった合衆国対ニューヨーク電話会社判決の際とは異なり、Apple社にとってパスコードを解除することは一般的な業務ではない。
4. Apple社はこれまで積極的にiPhoneのロック機能を回避するための情報を政府に提供したことはなく、その意向もない。Apple社は本件命令の適法性について争っているが、適法な命令には従うとしている。
5. ダイヤル先記録装置を装着することは簡単であるが、Apple社がロック機能回避の技術的支援を行うには、人的な負担を伴う。

暗号化と憲法

■端末の所有者や端末を使用していた被疑者自身にロック解除を命じることは合憲か?

- ロック手段、パスワードの種類によって異なると解されている
- 指紋等のバイオメトリック認証によってロックされている場合は、強制的に端末のロックを解除させることは可能

■ 連邦最高裁
- ●シュマーバー対カリフォルニア判決(1966年)
  - ◆物理的または肉体的な証拠を強制的に提出させること、特に指紋を採取することは、合衆国憲法修正5条に違反しない
- ●ドー対合衆国判決(1988年)
  - ◆被疑者に対して血液サンプルや筆跡を提供させること、被疑者の声を録音して証拠とすることは修正5条に違反しない

■ 端末所有者や使用者の指紋だけで端末がロックされている場合には、捜査機関は令状に基づき端末所有者や使用者の指紋を採取して、ロックを解除することが可能であり、このことは憲法には違反しない

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 連邦最高裁
- ●コンピューターや携帯電話等にパスワードを強制的に入力させることの合憲性については未判断
- ●1988年ドー対合衆国判決
  - ◆刑事事件の証拠物が入っている金庫の鍵の引き渡しを命じることはできるが、壁金庫(wall safe)のダイヤル鍵の解錠のために強制的に鍵の組み合わせを命じることはできない

■ 数字や記号、アルファベット等の組み合わせを命じることによってパスワードを強制的に端末に入力させることは、ドー判決に照らすと憲法違反か?

- 文字や記号、アルファベット等の組み合わせによって構成されるパスワードにも適用されると解するのであれば、強制的にそれらの組み合わせを命じることによってパスワードを強制的に端末に入力させることは憲法違反
- 指を物理的に動かしてパスワード等を入力させることは筆跡を提供させることと同じであり、許されると解する余地あり
- ただし、連邦控訴裁は、パスワードを強制的に入力させることは違憲と判断
- 合憲との説もあり

- 第11巡回区連邦控訴裁判所判決
  - 暗号化されたハードディスクを押収した際、所有者であった被疑者に対してそれを強制的に復号化させた
  - 捜査機関がハードディスク内部のデータにアクセスし、それを証拠として提出
  - 被告人側が修正5条違反であると主張
  - 「復号化させてハードディスクを提供させることは、容疑者の知性(mind)の内容を使用するものであり、単なる肉体的な行為とはいえない」 → 復号の強制は憲法違反
    - ◆United States v. Doe (In re Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1346 (11th Cir. Fla. 2012).

■Apple社、またはApple社の技術者には、技術的支援を拒む憲法上の権利があるか

- オーリン・カー(Orin Kerr)ジョージワシントン大学教授
  - ◆本件は、不合理な捜索及び逮捕・押収からの人民の権利の保障と令状主義を定める合衆国憲法修正4条の問題ではない
  - ◆2件の事案においてiPhoneの押収自体は令状に基づいて適法に行われている　→　令状に基づいて、政府側はApple社に対してその執行にあたって協力を求めることができる
  - ◆カリフォルニア事案では携帯電話の所有者の同意を得れば足りる
  - ◆カリフォルニア事案では被疑者が死亡　→　カー教授の所論を一般論として展開することができるかどうかには若干の疑問

Orin Kerr, *Preliminary Thoughts on the Apple iPhone Order in San Bernadino Case (Part 1),* https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/18/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-1/.

- ダン・テルジャン(Dan Terzian)弁護士
  - ◆iPhoneの製造販売者であるApple社は法人であるから、合衆国憲法修正5条による保障は及ばない
    - United States v. White, 322 U.S. 694, 698 (1944).
  - ◆デュー・プロセスの問題として、Apple社には本件における命令の適法性について異議を主張するための口頭審問を求める権利は存在
    - Dan Terzian, The Micro-Hornbook on the Fifth Amendment and Encryption, 104 GEO. WASH. L. J. ONLINE 168 (2016).
- ジャック・ゴーン(Jack Gohn)弁護士
  - ◆自然人であるApple社の従業員が技術的支援に同意していないにもかかわらず支援を行うことを命じるのは、当事者が適法に有罪判決を受けた犯罪に対する処罰の場合を除いて意に反する苦役を禁止する憲法修正13条違反の可能性
  - ◆被用者である従業員の権利を侵害する恐れがあるから、使用者であるApple社に対し技術的支援を命令することは、違法?

検討

- 2つの事案の性質の相違は、影響を与えているのか
- Apple社自身には憲法上の保護は及ぶか
  - 合衆国対電話会社判決の影響
  - 過重な負担?
  - セキュリティへの脅威?
  - Appleは、他の事例では協力しているのか
    （70件の端末ロック解除にすでに協力?）
  - iPhoneではなく、タブレット等の場合は?
- Googleに対するAndroid端末のパスワード開示命令との相違

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

今後の展望

■政府や捜査機関等がロックを解除したりデータを取り出したりすることができるように、あらかじめ製品を設計することを義務づけたり、ロック機能自体を禁止したりする法律を制定?

■「2016年裁判所命令遵守法案(Compliance with Court Orders Act of 2016)」

■上院情報委員会のリチャード・バー(Richard Burr)委員長(共和党)、ダイアン・ファインスタイン(Dianne Feinstein)議員(民主党)など有力議員が法案提出を準備

■2016年裁判所命令遵守法案
(Compliance with Court Orders Act of 2016)

- すべての通信事業及び製品(ソフトウェアを含む)の提供者は、適切なデータのセキュリティの実施を通じて合衆国の人民のプライバシーを保護しなければならず、法の支配を尊重しすべての法的要件と裁判所の命令を遵守しなければならない。(2条4項)
- 法の支配と合衆国の利益及びセキュリティの保護を実現するため、情報もしくはデータに関する裁判所の命令を受領したすべての者は、すみやかに、応答的かつ明確な(intelligible)情報もしくはデータ、または当該情報もしくはデータを取得するための適切な技術的支援を提供しなければならない。(同5項)
- 本法の適用を受ける団体は、裁判所の命令に基づき、応答的かつ明確な(intelligible)情報もしくはデータ、または当該情報もしくはデータを取得するための適切な技術的支援を政府に提供しなければならない(同6項)。

■「明確な(intelligible)」の定義(4条10項)。
- 情報もしくはデータに関する「明確な」とは、次の各号をいうものとする。
- (A)情報またはデータが、暗号化(encrypted)、秘密化(enciphered)、符号化(encoded)、モジュール化(modulated)、もしくは不明瞭化(obfuscate)されていないこと。
- (B)暗号化、秘密化、符号化、モジュール化もしくは不明瞭化された情報またはデータが、当初の状態に復号化(decrypted)、明瞭化(deciphered)、復元化(decoded)、非モジュール化(demodulated)、もしくは明瞭化(deobfuscated)されていること。

■OS自体に捜査機関等がロックを外すことのできる機能をあらかじめ組み込む、またはそもそもこのようなロック機能を装備することの要求は、禁止(3条(b))
- (b)デザインの制限　本法のいかなる文言も、本法の適用を受ける当事者に対し、特定のデザインもしくはオペレーティング・システムを採用することまたは禁止することをいかなる政府の官吏にも授権したものと解釈してはならない。

■クラウド

●(e)ライセンス供与者　リモートコンピューティング

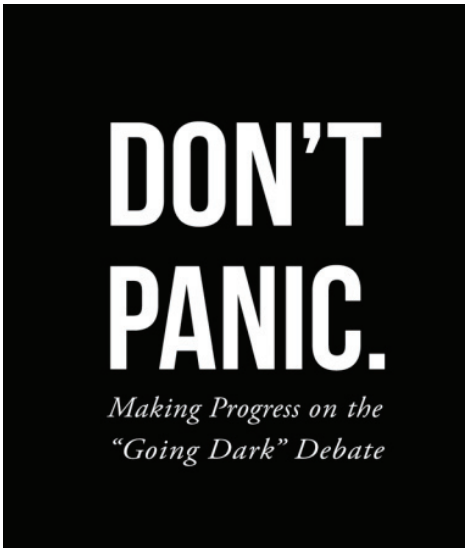
役務もしくは公衆電気通信の提供者であって、製品、サービス、アプリケーションもしくはソフトウェアのライセンスを本法の適用を受ける当事者に供与する者または当該当事者から供与される者は、ライセンスが供与された当該製品、サービス、アプリケーションもしくはソフトウェアが本法の規定に適合するようにしなければならない。

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

課題

アメリカ

- 安全保障やテロ対策とプライバシーとの相克
  - プライバシー・バイ・デザイン vs. フォレンジック・バイ・デザイン
- フォレンジック・バイ・デザインは、“Going Dark”なのか
  - ハーバード大学バークマン・インターネット及び社会センター“Don’t Panic.”（2016年2月）



https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

日本

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- ロック解除や復号の被疑者への強制
- デジタル・フォレンジック
  - 端末にインストールされているソフトウェア等の著作権その他の権利を侵害しないか（プロプライエタリ）
  - 端末上でソフトウェアを起動し、データを取得する方法の合法性
- 捜査機関で令状に基づき押収した端末のDFが困難な場合、ロック復号の支援等、技術的支援を令状に基づいて命令できるか
- 法改正等が必要か