法的手続きのガイドライン

日本とAPACの法執行機関

このガイドラインは、日本とアジア太平洋（以下「APAC」）地域の法執行機関またはその他の政府機関が、この地域でサービスを提供するApple関連企業に対し、Appleの製品およびサービスのユーザー、またはApple製デバイスに関する情報を要求する際に使用するためのものです。このガイドラインにおける「Apple」とは、Appleのプライバシーポリシー（ http://www.apple.com/jp/privacy/ ）に従って、特定の地域の顧客情報に対する責任を負う関連企業を指します。Appleは必要に応じてこのガイドラインを更新します。このバージョンは2015年9月29日に発行されたものです。

情報開示についてのユーザーの質問を含む、Appleのユーザーに関するその他すべての情報提供の要求は、https://www.apple.com/jp/privacy/contact/ で受け付けます。このガイドラインは、法執行機関が日本およびAPAC地域外のApple Inc.またはApple関連企業に対して情報提供を要求する場合には適用されません。

政府から情報提供を求められた場合、Appleは当社のデータを管理している全世界の企業に関する法令を遵守し、法的要求に準じて詳細を提供します。米国外の法執行機関によるコンテンツ提供の要求については、緊急事態（後出の「緊急対応要求」のセクションで定義）を除き、Appleは刑事共助条約にもとづく手続き、または米国司法省とのその他の協調的取り組みを通じて捜査令状が発行された場合にのみコンテンツを提供します。

索引

I. 一般情報

Appleは、モバイル通信およびメディアデバイス、パーソナルコンピュータ、ポータブルデジタル音楽プレーヤーを設計、製造、販売しています。また、これらに関連する様々なソフトウェア、サービス、周辺機器、ネットワーク接続ソリューション、他社製デジタルコンテンツおよびアプリケーションを販売しています。Appleの製品とサービスには、Mac、iPhone、iPad、iPod、Apple TV、コンシューマおよびプロ向けソフトウェアアプリケーションの製品ライン、iOSおよびMac OS Xオペレーティングシステム、iCloud、様々なアクセサリ、サービスおよびサポートの提供が含まれます。Appleはまた、iTunes Store、App Store、iBooks Store、Mac App Storeを通じて、デジタルコンテンツとアプリケーションを販売および提供しています。ユーザー情報は、Appleの プライバシーポリシー と、特定のサービスに適用されるサービス規約および利用規約 に従い、Appleによって保持されます。Appleは、Appleの製品とサービスのユーザーのプライバシー保護に全力で取り組んでいます。従って、Appleの製品とサービスのユーザー（以下「Appleユーザー」）に関する情報を、Appleが適切な法的手続きを経ることなく開示することはありません。

このガイドラインに含まれる情報は、日本とAPACの法執行機関に対し、これらの地域で法執行機関と政府機関に電子情報を開示するためにAppleが義務付けている法的手続きについての情報を提供するために作成したものです。このガイドラインは、法的な助言を提供するためのものではありません。このガイドラインの「よくある質問」のセクションは、Appleに多く寄せられる質問の一部に回答するためのものです。このガイドラインと「よくある質問」は、将来起こり得るすべての状況を網羅するものではありません。従って、その他の質問については、日本の法執行機関は japan_police_requests@apple.com 、APAC諸国の法執行機関は apac_police_requests@apple.com までお問い合わせください。これらのEメールアドレスの使用は、法執行機関と政府機関の職員に限定されます。このアドレスにEメールを送信する場合は、送信元が法執行機関の認証されたEメールアドレスであることが必要です。このガイドラインのいずれの内容も、Appleに対する法的強制力のある権利を付与するものではありません。また、Appleのポリシーは将来、法執行機関に通知することなく更新または変更される可能性があります。

Appleに対する法執行機関による要求の大半は、Appleの特定のデバイスまたはカスタマーと、Appleが当該カスタマーに提供し得る特定のサービスに関する情報を求めるものです。Appleは、要求された情報をAppleがその時点で所有している場合に限り、自らのデータ保持ポリシーに従って、Appleのデバイスまたはカスタマーの情報を提供できます。Appleは、後出の「Appleから入手可能な情報」セクションで概説している方法でデータを保持します。その他の全データは、当社の プライバシーポリシー に記載されている目的を果たすために必要な期間にわたり保持されます。法執行機関が情報提供を要求する際は、過度に広範な要求に対する誤解や異議の発生を避けるため、可能な限り具体的で的を絞った内容にしてください。

II. 法的文書の送達に関するガイドライン

A. 法執行機関による情報提供要求

Appleは、法執行機関による法的に有効な要求を、Eメールによって受理します。ただし、Eメールの送信元が、当該法執行機関の認証されたEメールアドレスであることを条件とします。日本とAPACの法執行機関職員がAppleに法的要求を提出する際は、日本では japan_police_requests@apple.com 宛て、APACでは apac_police_requests@apple.com 宛てに、認証された各法執行機関のEメールアドレスから直接送信してください。これらのEメールアドレスの使用は、法執行機関による要求の送信に限定されます。

Appleは、法執行機関が発行する法的手続き文書を有効と見なします。これには協力要請書（Cooperation Letter）、証拠入手通知（Notice of Obtaining Evidence）、召喚状、裁判所命令、捜査および差し押さえ令状、1979年オーストラリア電気通信法（Telecommunications Act of 1979）にもとづく委任状、または各地でこれらの有効な法的要求に相当する文書が該当します。Appleが必要とする文書の種類は国によって異なる場合があり、要求される情報によって種類が決定されます。

B. データ保存要求

Appleによって保存されるすべてのiCloudコンテンツデータは、サーバの設置場所において暗号化されます。データの保存に外部業者を使用する場合、Appleがその鍵を業者に渡すことは一切ありません。Appleは、米国の自社データセンターにおいて暗号鍵を保持します。従って、米国外の法執行機関が当該コンテンツを要求する際は、米国司法省の担当局を通じて法的手続きを進める必要があります。米国と刑事共助条約（MLAT）を締結している米国以外の国は、当条約で規定された手続き、または米国司法省担当局とのその他の協調的取り組みを通じて、適切な法的手続きを進めることができます。近々予定されているMLATの手続きの前にデータの保存を要求する場合は、Apple Inc.のEメールアドレス subpoenas@apple.com 宛てに要求を送信してください。データ保存要求を提出する際は、要求の真正性を確認できるように、文書内で特定されている機関名および職員名が記載された、法執行機関のレターヘッドを使用してください。文書にはEメールアドレスと電話番号を記載してください。

データ保存要求には、関連するApple ID/アカウントのEメールアドレス、または氏名と電話番号、および/または該当するAppleアカウントの氏名と住所を必ず記載してください。データ保存要求を受理した後、Appleは要求時に利用可能な既存のユーザーデータを一度抽出し、これを90日間保存します。この90日間が経過すると、保存されたデータはストレージサーバから自動的に削除されます。ただし、再度の要求を受けた場合は、この期間を90日間延長できます。同一アカウントの情報を3回以上保存する場合は、最初に保存された素材に対する延長要求として扱われ、Apple Inc.が当該要求に応じて新しい素材を保存することはありません。

C. 緊急対応要求

Appleは、以下の項目に対する深刻な脅威が真に差し迫っている状況に関連した要求を緊急対応要求と見なします。

1) 個人の生命または安全
2) 国家の安全
3) 極めて重要なインフラまたは施設に対する大規模な破壊行為

要求を行う法執行官が、上記の基準の1つ以上に該当する真の緊急事態に関する要求であることを十分に立証した場合、Appleはその要求を緊急に検討します。

Appleに緊急対応を要求する場合、要求を行う法執行官は付録Aに記載されている「EMERGENCY Law Enforcement Information Request」という名前のテンプレートに記入し、所属する法執行機関の認証されたEメールアドレスから exigent@apple.com 宛てに直接送信してください。その際、件名を「Emergency Law Enforcement Information Request」としてください。

Appleが「Emergency Law Enforcement Information Request」に応じてカスタマーデータを抽出する際は、これを提出した法執行機関職員の上司に連絡し、法執行機関による緊急の情報提供要求が正当であることの確認を求めます。「Emergency Law Enforcement Information Request」を提出する法執行機関職員は、要求を提出する際に、上司の連絡先情報を提供してください。

さらに、要求を行う法執行官が、AppleのGlobal Security Operations Center（GSOC）に電話（+1 408-974-2095）で連絡することもできます。法執行官がGSOCに電話をする際は、法執行機関が緊急に情報提供を求めている旨を伝えてください。さらに、要求の概要を説明し、適切なチームによる緊急対応要求としての対処が必要であることを伝えてください。この電話番号は全言語に対応しています。

D. アカウント削除要求

カスタマーのApple IDの削除をAppleに要求する場合、法執行機関は削除するアカウントと要求の根拠が明記された裁判所命令または令状をAppleに提供する必要があります。

III. Appleから入手可能な情報

A. デバイス登録

氏名、住所、Eメールアドレス、電話番号を含む基本的な登録情報またはカスタマー情報は、iOS 8とOS X Yosemite 10.10よりも前のApple製デバイスを登録する際に、カスタマーからAppleに提供されます。Appleはこの情報を検証しておらず、情報が正確ではない可能性や、デバイス所有者を反映していない可能性があります。iOS 8以降のバージョンを搭載したデバイスと、OS X Yosemite 10.10以降のバージョンを搭載したMacの登録情報は、カスタマーがデバイスをiCloudのApple IDと関連付けた時にAppleが受け取ります。この情報が正確ではない可能性や、デバイス所有者を反映していない可能性があります。登録情報は、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

Apple製デバイスのシリアル番号には「O」と「I」の英字が含まれないことに注意してください。Appleはシリアル番号に「0」と「1」の数字を使用します。「O」と「I」の英字を含むシリアル番号に関する要求には対応できません。

B. カスタマーサービス記録

デバイスまたはサービスについてカスタマーがAppleのカスタマーサービスとやり取りした記録を、Appleから入手できます。この情報には、Appleの特定のデバイスまたはサービスに関するカスタマーサポートコミュニケーションの記録が含まれる場合があります。さらに、デバイス、保証、修理に関する情報を利用できる場合もあります。この情報は、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

C. iTunes

iTunesは、カスタマーがデジタルミュージックとビデオを自分のコンピュータ上で管理および再生するために使用する、無料のソフトウェアアプリケーションです。また、カスタマーが自分のコンピュータまたはiOSデバイスにダウンロードできるコンテンツを提供するストアでもあります。カスタマーがiTunesアカウントを開設すると、登録者の氏名、住所、Eメールアドレス、電話番号などの基本情報が提供されます。さらに、iTunesで購入またはダウンロードした際の取引と接続の情報、iTunes登録者情報、IPアドレスの接続ログを、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

D. Apple Storeでの取引

Apple Storeで発生する店頭取引には、現金、クレジットカード、デビットカード、ギフトカードによる取引があります。特定の購入に関連したカードの種類、購入者の氏名、Eメールアドレス、取引日時、取引金額、店舗の場所に関する情報を入手するためには、法的に有効な要求が必要です。店頭取引記録に対する法的に有効な要求を提出する際は、使用されたクレジットカードまたはデビットカードの完全な番号と、取引日時、取引金額、購入商品などの追加情報を提供してください。さらに法執行機関は、レシートの写しを入手するために、購入に関連したレシート番号をAppleに提供できます。この情報は、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

E. Apple Online Storeでの購入

Appleは、氏名、配送先住所、電話番号、Eメールアドレス、購入した製品、購入金額、購入時のIPアドレスを含む、オンライン購入に関する情報を保持します。この情報を入手するためには、法的に有効な要求が必要です。オンライン注文（iTunesでの購入を除く）に関する情報提供を要求する際は、クレジットカードまたはデビットカードの完全な番号、注文番号、照会番号、または購入した製品のシリアル番号を提供してください。これらのデータと一緒にカスタマーの氏名を提供することもできますが、情報を入手するためにはカスタマーの氏名のみでは不十分です。この情報は、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

F. iTunes Card

iTunes Cardには、16桁の英数字で構成される引き替えコードが記載されています。このコードは、カード裏面に貼られている灰色のスクラッチシールの下に印字されています。また、カードの一番下には19桁のコードがあります。Appleはこれらのコードにもとづいて、カードがアクティベート済み[1]であるか、または使用済みであるかを特定できます。さらに、そのカードに関連付けられたアカウントにおける購入の有無も特定できます。iTunes Cardがアクティベートされると、Appleはアクティベートが行われた店舗、場所、日時を記録します。iTunes Storeでの購入によってiTunes Cardが使用されると、そのカードはユーザーアカウントに関連付けられます。この場合、登録者情報とIPアドレスを入手できる可能性があります。Apple Online Storeで購入されたiTunes Cardは、Apple Online Storeの注文番号によってAppleのシステムで探すことができます（注記：Appleを通じて購入されたiTunes Cardのみ。外部の小売業者を通じて購入されたiTunes Cardは除きます）。この情報は、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。法執行機関は、iTunes Cardの番号に関連して執行官が要求している正確な情報を提供する必要があります。

法執行機関または政府機関による法的手続きに応じて、AppleがiTunes Cardを無効化することはできません。

G. iCloud

iCloudは、自分が所有している音楽、写真、書類などにユーザーが自分のすべてのデバイスからアクセスできるようにする、Appleのクラウドサービスです。ユーザーのデジタルコンテンツの多くは、ユーザーのデバイス上だけでなく、クラウド上にも保存されています。そのためAppleは、Appleのエコシステム全体で、ユーザー情報の保護に注力しています。さらにiCloudは、カスタマーがiOSデバイスをiCloudにバックアップできるようにします。iCloudバックアップは、ユーザーが随時解除できます。カスタマーは、iCloudのサービスを使って、iCloud.comのEメールアカウントを取得できます。iCloudのEメールドメインには、@icloud.com、@me.com[2]、@mac.comがあります。Appleによって保存されるすべてのiCloudコンテンツデータは、サーバの設置場所において暗号化されます。データの保存に外部業者を使用する場合、Appleがその鍵を業者に渡すことは一切ありません。Appleは、米国の自社データセンターにおいて暗号鍵を保持します。

---

[1] 「アクティベート済み」とは、カードが小売業者の店頭で購入された後、一切使用されていない（iTunesアカウントの残高増額やiTunes Storeでのコンテンツ購入に使われていない）状態を指します。

[2] iCloudの開始に伴い、MobileMeサービスは廃止されました。従って、Appleは旧MobileMeアカウントと関連付けられた個々のコンテンツを保有していません。iCloudにないコンテンツは、現在保存されていません。

iCloudは登録式のサービスです。iCloudデータの提供を要求する際は、関連するApple ID/アカウントのEメールアドレスを必ず入れてください。Apple ID/アカウントのEメールアドレスが不明な場合、Appleは該当するAppleアカウントを特定するために、氏名と電話番号、および/または氏名と住所の形式の登録情報を必要とします。

iCloudから入手できる可能性がある情報は以下の通りです。

i. 登録者情報

カスタマーがiCloudアカウントを設定すると、氏名、住所、Eメールアドレス、電話番号などの登録者の基本情報がAppleに提供されます。さらに、iCloudの機能への接続に関する情報も利用できる場合があります。iCloud登録者情報とIPアドレスの接続ログは、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。接続ログは最大30日間保持されます。

ii. メールのログ

メールのログには、日時、送信者のEメールアドレス、受信者のEメールアドレスなど、受信および送信の通信記録が含まれます。執行官がメールのログを要求する場合は、その旨を法的要求に明記する必要があります。この情報は、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。iCloudのメールログは最大60日間保持されます。

iii. Eメールのコンテンツとその他のiCloudコンテンツ：フォトストリーム、書類、連絡先、カレンダー、ブックマーク、iOSデバイスのバックアップ

iCloudは、登録者のアカウントがアクティブな時に、登録者がアカウント内で保持することを選択したサービスのコンテンツのみを保存します。iCloudコンテンツには、Eメール、保存された写真、書類、連絡先、カレンダー、ブックマーク、およびiOSデバイスのバックアップが含まれる場合があります。iOSデバイスのバックアップには、ユーザーのカメラロールにある写真とビデオ、デバイス設定、アプリケーションデータ、iMessage、SMS、MMSメッセージとボイスメールが含まれる場合があります。Appleによって保存されるすべてのiCloudコンテンツデータは、サーバの設置場所において暗号化されます。データの保存に外部業者を使用する場合、Appleがその鍵を業者に渡すことは一切ありません。Appleは、米国の自社データセンターにおいて暗号鍵を保持します。米国外の法執行機関が当該コンテンツを要求する際は、米国司法省の担当局を通じて法的手続きを進める必要があります。米国と刑事共助条約（MLAT）を締結している米国以外の国は、当条約で規定された手続き、または米国司法省担当局とのその他の協調的取り組みを通じて、適切な法的手続きを進めることができます。Apple Inc.は、MLATの手続きに従って捜査令状が発行された場合にのみ、カスタマーのアカウントにあるカスタマーのコンテンツを提供します。

Appleは、Appleのサーバから消去された削除済みコンテンツを保持しません。

H. iPhoneを探す

「iPhoneを探す」は、ユーザー自身が有効にできる機能です。iCloudの登録者は、この機能を有効にすることにより、紛失した、または置き忘れたiPhone、iPad、iPod touch、Macを探すことができるほか、デバイスを紛失モードにする、デバイスをロックする、デバイス内のデータを消去するなどの特定の操作を行うことができます。このサービスの詳細については、http://www.apple.com/jp/icloud/find-my-iphone.html を参照してください。「iPhoneを探す」によって場所が特定されたデバイスの位置情報は、カスタマーに直接提供されます。Appleは、このサービスによって提供される地図またはEメールアラートの記録を持っていません。

「iPhoneを探す」の接続ログを利用できる可能性があります。このログは、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。「iPhoneを探す」の接続ログは、約30日間入手できます。

デバイスのリモートロック、またはデバイス内のデータ消去のリクエストがカスタマーによる操作である場合は、「iPhoneを探す」のトランザクションアクティビティを入手できる可能性があります。データのリモート消去についての情報は、要求者の国向けの適切な法的手続き文書が受理された場合にのみ入手できます。法執行機関からの要求に応じて、Appleがカスタマーのデバイス上でこの機能を有効にすることはできません。「iPhoneを探す」機能は、該当するデバイスに対して、カスタマーが事前に有効にしておく必要があります。Appleは、特定のデバイスのGPS情報を持っていません。

I. パスコードロックされたiOSデバイスからのデータ抽出

特定のデバイス上の特定のコンテンツにアクセスするための技術的なサポートを要求する場合は、刑事共助条約（MLAT）の手続きを通じてApple Inc.に連絡してください。米国外の法執行機関が当該コンテンツを要求する際は、米国司法省の担当局を通じて法的手続きを進める必要があります。米国とMLATを締結している米国以外の国は、当条約で規定された手続き、または米国司法省担当局とのその他の協調的取り組みを通じて、適切な法的手続きを進めることができます。

iOS 8.0以降のバージョンを搭載したすべてのデバイスについては、データ抽出ツールが機能しないため、AppleはiOSデータの抽出を行いません。抽出されるファイルは、ユーザーのパスコードに関連付けられた暗号鍵によって保護されています。Appleはこの暗号鍵を保有していません。

iOS 8.0よりも前のiOSバージョンを搭載したiOSデバイスについては、MLATの手続きに従って発行された捜査令状を受理した後、Apple Inc.がパスコードロックされたiOSデバイスから特定のカテゴリーのアクティブデータを抽出できます。具体的には、Appleのネイティブアプリケーションに含まれている、パスコードによってデータが暗号化されていないiOSデバイス上にあるユーザー生成アクティブファイル（以下「ユーザー生成アクティブファイル」）を抽出し、外部メディアの形式で法執行機関に提供できます。Apple Inc.は、iOS 4からiOS 7までを搭載したiOSデバイス上でこのデータ抽出プロセスを行うことができます。ただし、ユーザー生成アクティブファイルのうち、MLATの手続きによって発行された捜査令状を受理した後にApple Inc.が法執行機関に提供できるのは、SMS、iMessage、MMS、写真、ビデオ、連絡先、音声記録、通話履歴のカテゴリーに属するものです。Apple Inc.は、Eメール、カレンダーのエントリー、他社製アプリケーションのデータを提供できません。

正常に動作するデバイスについては、カリフォルニア州クパチーノにあるApple Inc.本社でのみデータ抽出プロセスを行うことができます。Apple Inc.がこのプロセスをサポートするためには、後出の文言を捜査令状に記載することが必要です。また、捜査令状にはデバイスのシリアル番号またはIMEI番号を必ず入れてください。iOSデバイスのシリアル番号またはIMEI番号の場所の詳細については、http://support.apple.com/kb/ht4061 を参照してください。

捜査令状に記載する裁判官の氏名は、書類に正しく記入できるように、はっきりと判読できる活字体で記載してください。

法執行機関は、この文言を含む捜査令状を取得した後、その令状を subpoenas@apple.com 宛てのEメールによってApple Inc.に送達してください。データを抽出するiOSデバイスをApple Inc.に渡す方法には、面会と配送があります。法執行機関が配送を選択した場合は、配送を依頼するAppleからのEメールを執行官が受信するまでは、デバイスを発送しないでください。

面会によって渡す場合、法執行機関職員は、iOSデバイスのメモリ容量の2倍以上にあたるストレージ容量があるFireWireハードドライブを持参してください。デバイスを配送する場合、法執行機関は、iOSデバイスのメモリ容量の2倍以上にあたるストレージ容量がある外部ハードドライブ、またはUSBサムドライブをAppleに提供してください。配送を依頼するEメールを受信するまでは、デバイスを発送しないでください。

データ抽出プロセスの完了後、デバイス上のユーザー生成コンテンツのコピーが提供されます。Apple Inc.は、このプロセスによって抽出されたユーザーデータのコピーを一切保持しません。従って、すべての証拠の保存は、法執行機関の責任のもとで行われるものとします。

捜査令状への記載が必要な文言：

> 「アクセス番号（電話番号）_____、シリアル番号[3]またはIMEI番号[4]_____、およびFCC ID番号_____を持つ、_____ネットワーク上のモデル番号_____のApple製iOSデバイス1台（以下「デバイス」）の捜査において、デバイスが正常に動作し、パスコードロックによって保護されている場合、Apple Inc.が妥当な技術的支援の提供によって[法執行機関]を支援することを、この書面をもって命ずる。この妥当な技術的支援には、可能な範囲におけるデバイスのデータ抽出、デバイスから外部ハードドライブまたはその他のストレージメディアへのデータのコピー、および前述のストレージメディアの法執行機関への返却が含まれる。法執行機関はその後、提供されたストレージメディア上にあるデバイスのデータの捜査を実施できるものとする。
>
> さらに、デバイス上のデータが暗号化されている場合、Appleは暗号化されたデータのコピーを法執行機関に提供できるが、その解読を試みることや、その他の方法で法執行機関が暗号化されたデータにアクセスできるように計らう義務はないものとする。
>
> Appleは、デバイス上のデータの完全性を維持するために妥当な努力をする一方で、この書面により命じられた支援の結果としてユーザーデータのコピーを保持する義務は一切ないものとする。従って、証拠の保存は法執行機関の責任のもとで行われるものとする。」

J. その他の入手可能なデバイス情報

MACアドレス：Mac（Media Access Control）アドレスは、物理的なネットワークセグメント上の通信用ネットワークインターフェイスに割り当てられる一意識別子です。Bluetooth、Ethernet、Wi-Fi、FireWireなどのネットワークインターフェイスを持つすべてのApple製品は、1つ以上のMACアドレスを持っています。MACアドレスは、シリアル番号（iOSデバイスの場合はIMEI、MEID、またはUDID）をAppleに提供し、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

UDID：UDID（Unique Device Identifier）は、各iOSデバイスに固有の、40の英数字で構成された文字列です。例えば「2j6f0ec908d137be2e1730235f5664094b831186」のようなものです。

---

[3] Apple製デバイスのシリアル番号には「O」と「I」の英字が含まれないことに注意してください。Appleはシリアル番号に「0」と「1」の数字を使用します。「O」または「I」の英字が含まれるシリアル番号のiOSデバイスからデータを抽出することはできません。

[4] IMEI番号は、携帯電話通信に対応しているiPad、初代iPhone、iPhone 5、iPhone 5c、iPhone 5s、iPhone 6、iPhone 6 Plusの背面に刻印されています。詳細については http://support.apple.com/kb/ht4061 をご覧ください。IMEI番号がSIMトレイに刻印されているモデルについては、デバイス内のSIMトレイが最初に付属していたトレイと異なる場合があるため、注意が必要です。

法執行機関がデバイスを所有している場合は、デバイスをiTunesに接続して、UDIDを入手できます。iTunesの「概要」タブの下にあるシリアル番号をクリックすると、UDIDが表示されます。

K. Apple Store監視ビデオ提供要求

ビデオ監視記録は、Apple Storeで最大30日間保持されます。この期間が経過すると、ビデオ監視記録を利用できない場合があります。法執行機関がビデオ監視記録の提供を要求する場合は、日本では japan_police_requests@apple.com 宛て、その他のAPAC地域では apac_police_requests@apple.com 宛てにEメールを送信してください。要求が受理された後、Eメールが適切なチームに転送され、処理されます。該当するデータがある場合は、担当チームが法執行機関職員に直接連絡します。

L. Game Center

Game CenterはAppleのソーシャルゲーミングネットワークです。ユーザーまたはデバイスのGame Centerへの接続に関する情報を利用できる場合があります。IPアドレスの接続ログとトランザクション記録は、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

M. iOSデバイスのアクティベーション

カスタマーがiOSデバイスをアクティベートするか、ソフトウェアをアップグレードした時は、そのイベントに応じて、特定の情報がサービスプロバイダまたはデバイスからAppleに提供されます。イベントのIPアドレス、ICCID番号、その他のデバイス識別子を利用できる場合があります。この情報は、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

N. サインオンのログ

iTunes、iCloud、My Apple ID、Apple DiscussionsなどのAppleのサービスに対するユーザーまたはデバイスのサインオンアクティビティを利用できる場合は、これをAppleから入手できます。IPアドレスの接続ログまたはサインオントランザクション記録は、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

O. My Apple IDとiForgotのログ

ユーザーのMy Apple IDおよびiForgotのログをAppleから入手できます。My Apple IDとiForgotのログには、パスワードリセットアクションに関する情報が含まれる場合があります。IPアドレスの接続ログまたはサインオントランザクション記録は、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

P. FaceTime

FaceTimeでのコミュニケーションは、エンドツーエンドで暗号化されます。FaceTimeデータがデバイス間で送受信されている間、Appleがそのデータを解読することはできません。また、FaceTimeでのコミュニケーションをAppleが傍受することもできません。Appleは、FaceTime通話への招待が開始された時に、FaceTime通話の招待ログを保持します。このログは、ユーザー間でのコミュニケーションの内容を示すものではありません。Appleは、FaceTime通話の確立の成功または失敗や、FaceTime通話の継続時間についての情報を保持しません。FaceTime通話の招待ログは最大30日間保持されます。FaceTime通話の招待ログは、要求者の国向けの適切な法的手続き文書を提出することによって入手できます。

IV. よくある質問

Q. 自分が所属する法執行機関からの情報提供要求や法的手続きについて、Appleに質問することはできますか?

A:はい。質問や問い合わせについては、日本では japan_police_requests@apple.com 宛て、APAC地域では apac_police_requests@apple.com 宛てにEメールを送信してください。

Q. ロックされているiOSデバイスのパスコードをAppleに提供してもらうことはできますか?

A:いいえ。Appleはユーザーのパスコードにアクセスできません。ただし、このガイドラインで説明している通り、デバイスに搭載されたiOSのバージョンによっては、MLATの手続きに従って発行された有効な捜査令状があれば、ロックされたデバイスからデータを抽出できる場合があります。

Q. Appleは要求に応じて提供できるGPS情報を保存していますか?

A:いいえ。Appleはデバイスのジオロケーションを追跡しません。

Q. 提供された情報を使って法執行機関が捜査または刑事事件に関する業務を完了した後、その情報はどのように処理すべきですか?

A:法執行機関のために抽出された、個人を特定できる情報を含むすべてのファイルと記録(すべてのコピーを含む)は、関連する捜査、犯罪事件に関する業務、すべての再審請求が完全に終了した後に必ず破棄してください。

Q. 盗難にあったデバイスや紛失されたデバイスを正当な所有者に返却する際に、サポートを依頼することはできますか?

A:紛失された、または盗難にあった疑いのあるデバイスを法執行機関が回収し、「元の所有者」への返却を試みる場合、日本の法執行機関は japan_police_requests@apple.com 宛て、APACの法執行機関は apac_police_requests@apple.com 宛てにEメールを送信し、登録情報を要求してください。Eメールには、デバイスのシリアル番号またはIMEI番号と、関連する追加情報を記載してください。登録情報を利用できる場合は、法執行機関が登録者に連絡し、デバイスが回収された旨を通知できるように、Appleがその情報を提供します。

V. 付録A

「EMERGENCY Law Enforcement Information Request」フォームは、次のリンクから編集可能なPDFとして入手できます。
http://www.apple.com/legal/privacy/le-emergencyrequest.pdf