法的手続きのガイドライン

米国外の政府と法執行機関

このガイドラインは、米国外の政府と法執行機関が、その地域または国のApple関連法人に対し、Appleのデバイス、製品、サービスの顧客に関する情報を請求する際に使用するためのものです。Appleは必要に応じてこのガイドラインを更新します。

このガイドラインにおける「Apple」とは、特定の地域または国で顧客情報に対する責任を負う関連法人を指します。Appleは、グローバル企業として様々な法域に法人を持ちます。これらの法人が収集する個人情報に対する責任は当該法人にあり、Apple Inc.はそうした情報の処理を代行しています。例えば、米国以外にあるAppleの小売事業体の店舗販売情報は、各国にあるAppleの個別の小売事業体が管理します。特定の法域におけるapple.comおよびAppleメディアサービス関連の個人情報も、各サービス規約に規定されている通り、米国外の法人が管理する場合があります。通常、米国外のApple法人でオーストラリア、カナダ、アイルランド、および日本にある法人は、それぞれの地域内でAppleが提供するサービスに関連する顧客データに対する責任を負っています。

Appleの顧客に関するその他のあらゆる情報提供請求は、情報開示に関する顧客からの質問を含め、www.apple.com/jp/privacy/contact/ で受け付けます。このガイドラインは、米国の政府と法執行機関がApple Inc.に対して行う請求には適用されません。

政府と法執行機関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法人に適用される法律を遵守し、法的に求められる通りに情報を提供します。米国外の政府と法執行機関からのコンテンツ提供の請求は、緊急事態（以下の「緊急の請求」セクションで定義）を除き、すべて米国のECPA（電子通信プライバシー保護法）を含む適用法に準拠している必要があります。刑事共助条約に基づく請求または海外データ合法的使用明確化法に定める行政協定（「クラウド法に定める協定」）に基づく請求は、ECPAに準拠するものとします。Appleは、このような法的に有効な手続きに基づく請求に対してのみ、顧客のアカウントにある通りに、顧客のコンテンツを提供します。

民間の当事者から請求があった場合、Appleは、顧客データを管理している現地の法人に適用される法律を遵守し、法的に求められる通りにデータを提供します。

Appleは、政府、法執行機関および民間の当事者からの正当な法的請求について、これを受領した時点から回答を提供する時点まで、その受領、追跡、処理、回答のプロセスを一元化しています。Apple

の法務部門の熟練したチームが、受領したすべての請求を検討し評価します。請求に有効な法的根拠がないとAppleが判断した場合、または請求が不明確、不適切、もしくは過度に広範であるとAppleがみなした場合、その請求に対して不服もしくは異議が申し立てられるか、その請求は拒否されます。

Appleは、請求を行った法執行機関に対して、請求を行った担当者の正式な法執行機関のメールアドレス宛てに回答を提供します。Appleが提供する回答に基づく証拠保全はすべて、請求を行う法執行機関の責任です。

索引

I. 一般的な情報

Appleは、モバイル通信とメディアデバイス、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、他社製のデジタルコンテンツと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 touch、Apple TV、Apple TV+、Apple Watch、HomePod、AirPods、AirTag、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macOS 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、Apple Music、App Store、Apple Books、および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。顧客情報は、Appleのプライバシーポリシーと、個々のサービスに適用されるサービス規約に従い、Appleによって保持されます。Appleは、Appleの製品とサービスの顧客（以下「Appleの顧客」）のプライバシー保護に全力で取り組んでいます。そのため、法律が定める緊急の状況を除き、Appleの顧客に関する情報が有効な法的手続きを経ることなく開示され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、米国外の政府と法執行機関に電子情報を開示するためにAppleが求める法的手続きについて、米国外の政府と法執行機関に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ことを意図していません。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。

その他の質問がある場合は、lawenforcement@apple.com までお問い合わせください。

上記のメールアドレスの使用は、政府と法執行機関の職員に限定されます。このアドレス宛てにメールを送信する場合は、送信元が政府または法執行機関の有効かつ正式なメールアドレスであることが必要です。

Appleに対する法的請求は、Appleの特定のデバイスまたは顧客と、Appleが当該顧客に提供できる特定のサービスに関する情報を求めるものである必要があります。Appleは、自らのデータ保持ポリシーに従って、請求された情報をAppleがその時点で保有している場合に限り、Appleのデバイスまたは顧客の情報を提供できます。Appleは、以下の「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。その他のデータはすべて、当社のプライバシーポリシーに記載されている目的を満たすために必要な期間にわたり保持されます。政府と法執行機関が情報提供を請求する際は、請求の内容が不明確、不適切、もしくは過度に広範であったために誤解、不服申し立て、異議申し立て、または拒否が発生するのを避けるため、可能な限り具体的かつ的を絞った内容にしてください。米国外の政府と法執行機関からのコンテンツ提供の請求は、緊急事態（以下の「緊急の請求」セクションで定義）を除き、すべて米国のECPA（電子通信プライバシー保護法）を含む適用法に準拠している必要があります。刑事共助条約に基づく請求または海外データ合法的使用明確化法に

定める行政協定（「クラウド法に定める協定」）に基づく請求は、ECPAに準拠するものとします。Appleは、このような法的に有効な手続きに基づく請求に対してのみ、顧客のアカウントにある通りに、顧客のコンテンツを提供します。

このガイドラインのいずれの内容も、Appleに対して行使でき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、政府または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。

II. Appleへの法的請求

A. 政府と法執行機関からの情報提供請求

Appleは、政府または法執行機関からの法的に有効な情報提供請求を、政府または法執行機関からのメールによって受領します。ただし、送信元が請求を行う政府または法執行機関の正式なメールアドレスであることを条件とします。米国外の政府と法執行機関の職員がAppleに情報提供請求を提出する際は、「Government & Law Enforcement Information Request」テンプレートに記入して、当該政府または法執行機関の正式なメールアドレスから、lawenforcement@apple.com 宛てに直接送信してください。

上記のメールアドレスの使用は、政府と法執行機関の職員に限定されます。デバイスのシリアル番号やIMEI番号、Apple ID、メールアドレス、請求書番号や注文番号など、5つ以上の識別子が請求に含まれる場合は、編集可能な形式で送信してください（Numbers、Excel、Pages、Wordなどの文書）。通常、このような識別子が、デバイス、アカウント、または支払い処理のいずれかに関連する情報を探すために必要となります。

注意：システムのセキュリティ基準により、Appleが、メールで提出されたリンクから法的請求または関連する文書をダウンロードすることはありません。

法執行機関からの請求に対してAppleが顧客情報を開示するためには、法執行機関がAppleなどのデータ管理者から個人データの形式で証拠となる情報を収集する権限の法的根拠を、請求を行う担当者が示すことが必要です。Appleが法的に有効とみなす請求には、例えばProduction Orders（オーストラリア、カナダ、ニュージーランド）、lettres de réquisition ou commissions rogatoires（フランス）、Solicitud Datos（スペイン）、Ordem Judicial（ブラジル）、Auskunftsersuchen （ドイツ）、Obligation de dépôt （スイス）、個人情報の開示依頼（日本）、Personal Data Request, Orders, Warrants and Communications Data Authorisations（英国）、およびその他の国からの、これらに相当する裁判所命令または請求などがあります。

B. 政府と法執行機関からの情報提供請求の管理と対応

Appleは、各請求について正当な法的根拠があることの確実を期すため、すべての法的請求を慎重に確認し、法的に有効な請求に従います。請求に有効な法的根拠がないとAppleが判断した場合、または請求が不明確、不適切、もしくは過度に広範である場合、Appleはその請求に不服もしくは異議を申し立てるか、その請求を拒否します。

処理上の目的およびシステム上の制限を理由として、Appleは、25個を超えるアカウント識別子を含む法的請求を受け入れることはできません。法執行機関が25個を超えるアカウント識別子を含む法的請求を提出する場合、Appleは、最初の25個に対応するものとし、法執行機関は残りの識別子について新たな法的請求を再提出する必要があります。

C. データ保存請求

米国外の政府と法執行機関からのコンテンツ提供の請求は、緊急事態（以下の「緊急の請求」セクションで定義）を除き、すべて米国のECPA（電子通信プライバシー保護法）を含む適用法に準拠している必要があります。刑事共助条約に基づく請求または海外データ合法的使用明確化法に定める行政協定（「クラウド法に定める協定」）に基づく請求は、ECPAに準拠するものとします。間近にECPAに従った請求を予定しており、その前にあらかじめデータの保存を請求する場合は、メールで lawenforcement@apple.com 宛てに請求を送信してください。
データ保存請求には、関連するApple ID／アカウントのメールアドレス、または氏名**と**電話番号、または対象となるAppleアカウントの顧客の氏名**と**住所を必ず記載してください。データ保存請求を受領したあと、Appleは請求の時点で入手可能な請求された既存の顧客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、再度の請求を受けた場合は、一度に限り、この期間を90日間延長できます。
同じアカウントについて2つを超えるデータ保存請求の提出を試みた場合、2つ目の請求は元のデータ保存を延長するための請求として取り扱われることになり、別途新たなデータが保存されるための請求として取り扱われることはありません。

D. 緊急の請求

Appleは、ある請求が、個人の生命／安全に対する差し迫った重大な脅威、国家の安全、または重要なインフラストラクチャー／設備のセキュリティに関連するものである場合、当該請求を緊急の請求とみなします。

請求を行う政府または法執行機関の担当者が、上記の基準の1つ以上に該当する緊急事態に関する請求であることを十分に立証した場合、Appleはその請求に緊急に対応します。

Appleが緊急かつ自発的に情報を開示することを請求するためには、請求を行う政府または法執行機関の担当者は「Emergency Government & Law Enforcement Information Request」フォームに記入し、所属する政府または法執行機関の正式な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、件名に「Emergency Request」という用語を含めてください。

政府または法執行機関が「Emergency Government & Law Enforcement Information Request」に応じた顧客データを求める場合、これを提出した政府または法執行機関の担当者の上司に連絡がなされ、緊急の情報提供請求が正当であることをAppleに対して確認するよう求められる場合があります。「Emergency Government & Law Enforcement Information Request」を提出する政府または法執行機関の担当者は、請求を提出する際に、上司の連絡先情報を提供してください。

政府または法執行機関が緊急の問い合わせをするためにAppleに連絡する必要がある場合は、Appleの Global Security Operations Center（GSOC）（001 408 974-2095）まで連絡してください。この電話番号は複数の言語に対応しています。

E. アカウントの制限／削除請求

政府または法執行機関が顧客のApple IDの制限／削除をAppleに請求する場合、Appleは、制限／削除対象のアカウントが違法に使用されたことを証明する、裁判所命令またはその国におけるこれと同等のその他の法的手続き文書（多くの場合、有罪判決または令状）を必要とします。

Appleは、政府と法執行機関からのすべての請求を慎重に検討し、各請求に有効な法的根拠があるかどうかを確認します。請求に有効な法的根拠がないとAppleが判断した場合、または制限／削除対象のアカウントが違法に使用されたことを裁判所命令が証明していない場合、Appleはその請求に対する異議を申し立てるか、その請求を拒否します。

Appleが政府または法執行機関から受け取った裁判所命令またはその国におけるこれと同等のその他の法的手続き文書（多くの場合、有罪判決または令状）が、制限／削除対象のアカウントが違法に使用されたことを十分に証明している場合、Appleは裁判所命令に従ってアカウントを制限／削除するために必要な措置を講じ、請求を行った担当者にその旨を通知します。

F. 顧客への通知

Appleは、政府または法執行機関からの有効な法的請求によって顧客のAppleアカウントに関する情報の開示が求められた場合、その旨を当該顧客に通知します。ただし、その有効な法的請求、Appleが受け取った裁判所命令もしくは適用法により通知が明示的に禁止される場合、または通知によって特定可能な個人に傷害もしくは死亡の危険が生じるとAppleがその独自の裁量により判断する場合、児

童を危険にさらすことに関わる場合、もしくは背景事情を考慮すると通知が適切ではない場合を除きます。

緊急の情報開示がある場合、Appleは90日後にその旨を顧客にあとから通知します。ただし、裁判所命令もしくは適用法により通知が禁止される場合、通知によって特定可能な個人もしくはグループに傷害もしくは死亡の危険が及ぶ可能性があるとAppleが独自の裁量により判断する場合、または児童を危険にさらすことに関わる場合を除きます。Appleは、裁判所命令で指定された非開示期間の満了後に、その旨をあとから顧客に通知します。ただし、通知によって特定可能な個人もしくはグループに傷害もしくは死亡の危険が及ぶ可能性があるとAppleが独自の裁量により合理的に判断する場合、児童を危険にさらすことに関わる場合、または背景事情を考慮すると通知が適切ではない場合を除きます。

Appleは、制限／削除対象となるアカウントが違法に使用されたこと、またはAppleのサービス規約に違反して使用されたことを証明する裁判所命令（多くの場合、有罪判決または令状）をAppleが受領した結果として、顧客のAppleアカウントの制限／削除をした場合、その旨を当該顧客に通知します。ただし、法的手続き自体、Appleが受領した裁判所命令もしくは適用法により通知が禁止される場合、児童を危険にさらすことに関わる場合、通知によって特定可能な個人もしくはグループに傷害もしくは死亡の危険が生じる可能性があるとAppleが独自の裁量により判断する場合、または背景事情を考慮すると通知が適切ではない場合を除きます。

III. Appleから入手可能な情報

このセクションでは、このガイドラインの公開時点において、Appleから入手できる一般的な情報の種類について説明します。

A. デバイスの登録情報

氏名、住所、メールアドレス、および電話番号を含む基本的な登録情報または顧客情報は、iOS 8とmacOS Sierra 10.12よりも前のApple製デバイスを登録する際に、顧客からAppleに提供されています。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、macOS Sierra 10.12以降のバージョンを搭載したMacの登録情報は、顧客がデバイスをiCloudのApple IDと関連付ける際にAppleに送られます。この情報は、正確ではなかったり、デバイス所有者を反映していなかったりする可能性があります。登録情報がある場合、請求者の国において適切かつ法的に有効な請求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ご注意ください。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」の英字を含むシリアル番号に関する請求には対応できません。法的請求にシリアル番号が5つ以上含まれる場合、Appleは、これらのシリアル番号を編集可能な電子的形式で送信することも求めます（Numbers、Excel、Pages、Wordなどの文書）。

B. 顧客サービスの記録

デバイスまたはサービスについて顧客がAppleの顧客サービスとやり取りした記録を、Appleから入手できる場合があります。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顧客との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、保証および修理に関する情報がある場合もあります。こうした情報がある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

C. Appleメディアサービス

App Store、Apple Music、Apple TVアプリケーション、Apple PodcastおよびApple Books（以下「Appleメディアサービス」）は、顧客がアプリケーション、デジタルミュージックおよびビデオを整理および再生し、コンテンツをストリーミングするために使用するソフトウェアアプリケーションです。Appleメディアサービスは、顧客が自分のコンピュータおよびiOSデバイスにダウンロードするコンテンツも提供します。顧客がAppleアカウントを開設する際、顧客の氏名、住所、メールアドレス、電話番号などの基本的な顧客情報が顧客から提供される可能性があります。さらに、Appleメディアサービスで購入／ダウンロードした際の取引と接続に関する情報、アップデート／再ダウンロードした際の接続情報も存在する場合があります。IPアドレス情報は、直近18か月間のものに限られる可能性があります。Appleメディアサービスの顧客情報およびIPアドレスを含む接続ログがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

Appleメディアサービスのデータの提供を請求する際は、Appleのデバイス識別子（シリアル番号、IMEI、MEIDもしくはGUID）または関連するApple ID／アカウントのメールアドレスを必ず提供してください。Apple ID／アカウントのメールアドレスが不明な場合、該当するAppleメディアサービスの顧客アカウントを特定するために、Appleメディアサービスの顧客情報を氏名**と**電話番号、または氏名**と**住所という組み合わせでAppleに提供する必要があります。政府または法執行機関の担当者は、有効なAppleメディアサービスの注文番号、またはAppleメディアサービスでの購入に関連付けられたデビットカードまたはクレジットカードの完全な番号を提供することもできます。こうしたパラメータと顧客の氏名を組み合わせて提供することもできますが、情報を入手するためには顧客の氏名だけでは不十分です。

注意：法的請求にクレジットカード／デビットカードの完全なデータが含まれる場合、データの安全のため、クレジットカード／デビットカードのデータはパスワード保護または暗号化された文書（PDF、およびNumbers、Excel、Pages、Wordなどの編集可能な形式の文書）でlawenforcement@apple.com 宛てに送信し、そのパスワードを別のメールで送信してください。また、システムのセキュリティ基準により、Appleが、メールで提供されたリンクから法的請求の文書をダウンロードすることはありません。

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。店頭取引記録を請求する際は、使用されたクレジットカード／デビットカードの完全な番号を必ず提供してください。取引日時、金額、購入商品などの追加情報も提供することができます。特定の購入に関連するカードの種類、購入者の氏名、メールアドレス、取引日時、取引金額、および店舗の場所に関する情報がある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

レシートの写しを請求する際は、購入に関連する小売取引番号を必ず提供してください。入手可能な場合、請求者の国において適切かつ法的に有効な請求によってこれを入手できます。

注意：法的請求にクレジットカード／デビットカードの完全なデータが含まれる場合、データの安全のため、クレジットカード／デビットカードのデータはパスワード保護または暗号化された文書（PDF、およびNumbers、Excel、Pages、Wordなどの編集可能な形式の文書）でlawenforcement@apple.com 宛てに送信し、そのパスワードを別のメールで送信してください。また、システムのセキュリティ基準により、Appleが、メールで提供されたリンクから法的請求の文書をダウンロードすることはありません。

E. apple.comでの注文

Appleは、apple.comでのオンライン注文に関する情報を保持しており、これには購入者の氏名、配送先住所、電話番号、メールアドレス、購入製品、購入金額、購入時のIPアドレスなどが含まれる場合があります。apple.comでのオンライン注文に関する情報提供を要求する際は、クレジットカード／デビットカードの完全な番号もしくは注文番号、または購入した製品のシリアル番号のいずれかを必ず提供してください。これらのパラメータと顧客の氏名を組み合わせて提供することもできますが、情報を入手するためには顧客の氏名だけでは不十分です。あるいは、apple.comでのオンライン注文に関する情報提供を請求する際に、関連するApple ID／アカウントのメールアドレスを提供することもできます。Apple ID／アカウントのメールアドレスが不明な場合、Appleは、対象となるAppleアカウントを特定するために、顧客の氏名**と**電話番号、または氏名**と住所**という組み合わせで顧客情報を必要とします。apple.comでのオンライン注文に関する購入情報がある場合、
請求者の国において法的に有効な請求によって入手できます。

注意：法的請求にクレジットカード／デビットカードの完全なデータが含まれる場合、データの安全のため、クレジットカード／デビットカードのデータはパスワード保護または暗号化された文書（PDF、およびNumbers、Excel、Pages、Wordなどの編集可能な形式の文書）でlawenforcement@apple.com 宛てに送信し、そのパスワードを別のメールで送信してください。また、システムのセキュリティ基準により、Appleが、メールで提供されたリンクから法的請求の文書をダウンロードすることはありません。

F. ギフトカード

Apple StoreギフトカードおよびApp Store & iTunesギフトカードには、シリアル番号があります。シリアル番号は、デザインまたは発行日などによって形式が異なります。Appleは、Apple Storeギフトカードおよび App Store & iTunesギフトカードに関する情報が存在する場合、請求者の国において適切かつ法的に有効な請求に応じてこれを提供することができます。法的請求にギフトカードのシリアル番号が5つ以上含まれる場合、Appleは、これらのギフトカードのシリアル番号を、パスワード保護または暗号化された文書（Numbers、Excel、Pages、Wordなどの文書）でlawenforcement@apple.com 宛てに送信し、そのパスワードを別のメールで送信することを求めます。

i. Apple Storeギフトカード

Apple Storeギフトカードは、apple.comまたはApple Storeでの購入に利用できます。記録がある場合、記録にはギフトカード購入者の情報（第三者であるマーチャントではなくAppleから購入した場合）、関連する購入取引、および購入製品が含まれる場合があります。該当するカードのステータスによっては、AppleがApple Storeギフトカードをキャンセルまたは停止できる場合もあります。Apple Storeギフトカードに関する情報がある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

注意：法的請求にApple Storeギフトカードの完全なデータが含まれる場合、データの安全のため、Apple Storeギフトカードのデータはパスワード保護または暗号化された文書（PDF、およびNumbers、Excel、Pages、Wordなどの編集可能な形式の文書）でlawenforcement@apple.com 宛てに送信し、そのパスワードを別のメールで送信してください。また、システムのセキュリティ基準により、Appleが、メールで提供されたリンクから法的請求の文書をダウンロードすることはありません。

ii. App Store & iTunesギフトカード

App Store & iTunesギフトカードは、Apple Music、App Store、Apple Books、およびMac

App Storeで利用できます。Appleは、シリアル番号があればこれに基づいて、App Store & iTunesギフトカードがアクティベート済みであるか（小売業者の店頭で購入されたか）、または引き換え済みであるか（Appleアカウントの残高に反映されているか）を特定できます。

App Store & iTunesギフトカードがアクティベート済みで、記録がある場合、記録にはアクティベートが行われた店舗名、場所、および日時が含まれる場合があります。App Store & iTunesギフトカードが引き換え済みで、記録がある場合、記録には関連するAppleアカウントの顧客情報、アクティベーションまたは引き換えの日時、ならびに引き換え時のIPアドレスが含まれる場合があります。該当するカードのステータスによっては、AppleがApp Store & iTunesギフトカードを無効にすることができる場合もあります。App Store & iTunesギフトカードに関する情報がある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

注意：法的請求にApp Store & iTunesギフトカードの完全なデータが含まれる場合、データの安全のため、App Store & iTunesギフトカードのデータはパスワード保護または暗号化された文書（PDF、およびNumbers、Excel、Pages、Wordなどの編集可能な形式の文書）でlawenforcement@apple.com 宛てに送信し、そのパスワードを別のメールで送信してください。また、システムのセキュリティ基準により、Appleが、メールで提供されたリンクから法的請求の文書をダウンロードすることはありません。

G. Apple Pay

販売店で行われたApple Payでの取引（NFC／非接触でのやり取りなど）およびアプリケーション内またはオンラインのPOSで行われたApple Payでの取引は、顧客のデバイスで安全に認証され、暗号化された形式でマーチャントまたはマーチャントの決済代行会社に送信されます。取引のセキュリティはAppleのサーバによって検証されていますが、Appleは、支払いを処理せず、そうした取引または Apple Payを使用して行われた購入に関連付けられているクレジットカード／デビットカードの完全な番号を保存しません。こうした情報は、関連する発行金融機関、決済ネットワーク、またはマーチャントを通じて入手できます。

Apple Payに対応している国や地域に関する詳細は、support.apple.com/ja-jp/HT207957 で確認できます。

Apple Storeの店舗またはapple.comで行われた購入の取引データを請求する場合、Appleは、取引に使われたデバイスプライマリアカウント番号（DPAN）を必要とします。DPANは16桁で、発行銀行から取得できます。注意：DPANとは、マーチャントとの非接触型の支払い取引において、実際のクレジットカード／デビットカードの番号（FPAN／Funding PAN）の代わりに使用されるものです。DPANは、決済代行会社によって、対応するFPANに変換されます。関連するDPAN情報が提供されると、Appleは、そのPOSシステムを通じて対応する情報を特定するための合理的な検索を実施できる

場合があります。こうした記録がある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

Appleは、顧客がApple Payに追加したクレジットカード／デビットカードの種類に関するApple Payの情報および顧客情報を提供できる場合があります。こうした情報がある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。そうした情報を請求する場合、Appleは、デバイス識別子（Appleのシリアル番号、SEID、IMEI、もしくはMEID）またはApple ID／アカウントのメールアドレスを必要とします。

注意：法的請求にDPANが含まれる場合、データの安全のため、そのデータはパスワード保護または暗号化された文書（PDF、およびNumbers、Excel、Pages、Wordなどの編集可能な形式の文書）で lawenforcement@apple.com 宛てに送信し、そのパスワードを別のメールで送信してください。また、システムのセキュリティ基準により、Appleが、メールで提供されたリンクから法的請求の文書をダウンロードすることはありません。

H. iCloud

iCloudは、顧客が自分の写真やドキュメントなどに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。さらに、iCloudによって、顧客は自分のiOS／iPadOSデバイスのバックアップをiCloudに作成できます。顧客は、iCloudのサービスを使って、icloud.comのメールアカウントを設定できます。iCloudのメールドメインには、@icloud.com、@me.com、@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。Appleが復号できるデータについては、Appleは米国の自社データセンターで暗号鍵を保持します。Appleが、顧客のエンドツーエンドで暗号化されたデータの暗号鍵を受け取ったり、保持したりすることはありません。

iCloudは顧客ベースのサービスです。iCloudデータの提供を請求する際は、関連するApple ID／アカウントのメールアドレスを必ず提供してください。Apple ID／アカウントのメールアドレスが不明な場合、Appleは、対象となるAppleアカウントを特定するために、顧客の氏名**と**電話番号、または氏名**と**住所という組み合わせで顧客情報を必要とします。電話番号またはApple ID／アカウントのメールアドレスのみが提供された場合、それらの基準に関連付けられている検証済みのアカウントに関して入手できる情報が提示される場合があります。

I. iCloudから入手できる情報は以下の通りです。

I. 顧客情報

顧客がiCloudアカウントを設定すると、氏名、住所、メールアドレス、電話番号などの基本

的な顧客情報がAppleに提供される場合があります。さらに、iCloudの機能への接続に関する情報もある場合があります。iCloud の顧客情報およびIPアドレスを含む接続ログがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。接続ログは最長25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、送信者のメールアドレス、受信者のメールアドレスなど、送受信の通信記録が含まれます。iCloudのメールログは最長25日間保持されます。メールログがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

III. メールの内容およびその他のiCloudコンテンツ、マイフォトストリーム、iCloud写真、iCloud Drive、連絡先、カレンダー、ブックマーク、Safariの閲覧履歴、マップの検索履歴、メッセージ、iOSデバイスのバックアップ

iCloudでは、顧客のアカウントがアクティブである間、その顧客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が保存されます。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。iCloudコンテンツには、メール、保存された写真、ドキュメント、連絡先、カレンダー、ブックマーク、Safariの閲覧履歴、マップの検索履歴、メッセージ、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、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、Business Chat、SMS、および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。Appleが復号できるデータについては、Appleは米国の自社データセンターで暗号鍵を保持します。Appleが、顧客のエンドツーエンドで暗号化されたデータの暗号鍵を受け取ったり、保持したりすることはありません。

米国外の政府と法執行機関からのコンテンツ提供の請求は、緊急事態（前述の「緊急の請求」セクションで定義）を除き、すべて米国のECPA（電子通信プライバシー保護法）を含む適用法に準拠している必要があります。刑事共助条約に基づく請求または海外データ合法的使用明確化法に定める行政協定（「クラウド法に定める協定」）に基づく請求は、ECPAに準拠するものとします。Appleは、このような法的に有効な請求に対してのみ、顧客のアカウントにある通りに、顧客のコンテンツを提供します。

II.高度なデータ保護

iCloudの高度なデータ保護は、エンドツーエンドの暗号化を使用して、Appleの最高水準のデータセキュリティでiCloudデータを保護する機能です。iCloudの高度なデータ保護を有効に

しているユーザーについては、入手できるiCloudデータが限られる場合があります。高度なデータ保護の詳細は、support.apple.com/ja-jp/guide/security/advanced-data-protection-for-icloud-sec973254c5f/のウェブおよび support.apple.com/ja-jp/HT212520 で確認できます。

ユーザーがiCloudの高度なデータ保護を有効にしている場合にiCloudから入手できる可能性がある情報は以下の通りです。

a. 顧客情報
顧客がiCloudアカウントを設定すると、氏名、住所、メールアドレス、電話番号などの基本的な顧客情報がAppleに提供される場合があります。さらに、iCloudの機能への接続に関する情報もある場合があります。iCloudの顧客情報およびIPアドレスを含む接続ログがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。接続ログは最長25日間保持されます。

b. メールのログ
メールのログには、日時、送信者のメールアドレス、受信者のメールアドレスなど、送受信の通信記録が含まれます。iCloudのメールログは最長25日間保持されます。メールログがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

c. メールの内容およびその他のiCloudコンテンツ
高度なデータ保護を有効にしているユーザーについては、その顧客のアカウントがアクティブである間、顧客がアカウント内で保持することを選択したメール、連絡先、カレンダーのコンテンツがiCloudに保存されます。このデータは、顧客のアカウントに存在する場合、請求者の国において適切かつ法的に有効な請求によって提供できる可能性があります。この限られたデータはAppleによって保管され、サーバの設置場所において付加的な暗号化が行われます。Appleが復号できるデータについては、Appleは米国の自社データセンターで暗号鍵を保持します。Appleが、顧客のエンドツーエンドで暗号化されたデータの暗号鍵を受け取ったり、保持したりすることはありません。

高度なデータ保護ではエンドツーエンドの暗号化が使用されており、Appleは、写真、iCloud Drive、バックアップ、メモ、Safariブックマークといった特定のiCloudコンテンツを復号できません。状況によっては、AppleはこうしたiCloudサービスに関する限られた情報を保持し、そのような情報がある場合には、請求者の国において適切かつ法的に有効な請求によって入手できます。

III. iCloudプライベートリレー

iCloudプライベートリレーは、iCloud+サブスクリプションの一部として提供されるインター

ネットプライバシーサービスです。プライベートリレーは、Safariでのユーザーのウェブ閲覧、DNS（ドメインネームスペース）解決クエリ、アプリケーションの暗号化されていないHTTPトラフィックを保護します。iCloudプライベートリレーを利用するには、iCloud+サブスクリプションと、iOS 15、iPadOS 15、またはmacOS Monterey（macOS 12）以降を搭載したデバイスが必要です。プライベートリレーの詳細は、support.apple.com/ja-jp/HT212614 およびwww.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF で確認できます。

プライベートリレーが有効になっている場合、ユーザーのウェブ閲覧リクエストは、2つの個別の安全なインターネットリレーに分けて送られます。ユーザーのネットワークプロバイダと、Appleが運用する最初のリレーでは、ユーザーのIPアドレスを見ることができます。ユーザーのDNSレコードは暗号化されるため、ネットワークプロバイダもAppleも、ユーザーがアクセスしようとしているウェブサイトのアドレスを見ることはできません。2つ目のリレーは、他社のコンテンツプロバイダが運用しています。このプロバイダが一時的なIPアドレスを生成し、ユーザーが要求したウェブサイトの名前を復号して、ユーザーをそのサイトに接続します。プライベートリレーは、接続しているクライアントがiPhone、iPad、またはMacであることを検証します。プライベートリレーでは、ユーザーの元のIPアドレスを、サービスで使用されるIPアドレスの範囲から割り当てたアドレスに置き換えます。割り当てられたリレーIPアドレスは、同じ地域内の複数のプライベートリレーユーザー間で共有されます。

ユーザーのウェブ閲覧リクエストでプライベートリレーが使用されている場合、Appleがプライベートリレーの IPアドレスから、ユーザーのクライアントIPアドレスや対応するユーザーアカウントを特定することはできません。プライベートリレーのIPアドレスに関連付けられたApple IDについて、Appleが提供できる情報はありません。

注意：iCloudプライベートリレーは、一部の国や地域では利用できません。プライベートリレーを有効にしているユーザーが、プライベートリレーを利用できない場所に旅行した場合、プライベートリレーは自動的にオフになり、この機能を利用できる国や地域に再度入ると再びオンになります。

I. 「探す」

「探す」は、ユーザー自身が有効にできる機能です。iCloudの顧客は、この機能を有効にすることにより、紛失した、または置き忘れた自分のiPhone、iPad、iPod touch、Apple Watch、AirPods、Mac、AirTag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、デバイス上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は、www.apple.com/jp/icloud/find-my/ で確認できます。

デバイスを紛失した顧客が「探す」機能を使用するには、紛失前にその特定のデバイスで当該機能を有効にしておく必要があります。遠隔操作で、またはデバイスを紛失したあとに、または政府もしく

は法執行機関からの請求を受けてから、デバイスの「探す」機能を有効にすることはできません。デバイスの位置情報サービスの情報は個々のデバイス上に保存され、Appleが特定のデバイスからこの情報を取得することはできません。「探す」機能によって場所が特定されるデバイスの位置情報サービスの情報は、顧客に対して提供されるものであり、Appleは、このサービスを通じて送信される地図やアラートのコンテンツを保持していません。iOSデバイスの紛失または盗難があった場合に関する情報と顧客が実行できる手順は、support.apple.com/ja-jp/HT201472 で確認できます。

「探す」の接続ログが保存されるのは最長25日間で、接続ログがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。デバイスのリモートロック、またはデバイス上のデータ消去のリクエストに関する「探す」のトランザクションアクティビティがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

J. AirTagおよび「探す」ネットワーク対応アクセサリプログラム

iPhone、iPad、iPod touch、Macの「探す」アプリケーションを使うと、AirTagを取りつけた持ち物の場所や、「探す」ネットワーク対応アクセサリプログラムに含まれる製品の場所を特定することができます。

ユーザーはAirTag、iOS 14.5以降、macOS 11.3以降で「探す」アプリケーションを使って、紛失した持ち物を探すことができます（鍵、バックパック、スーツケースなど）。AirTagで音を鳴らす、または対応するiPhoneモデルで「正確な場所を見つける」を使用するには、AirTagが、ペアリングしたiPhone、iPad、iPod touchのBluetoothの通信範囲内にある必要があります。AirTagが持ち主の近くにない場合でも、世界中にある数億台のAppleデバイスで構成される「探す」ネットワークの通信範囲内にあれば、そのAirTagのおおよその位置は確認できます。詳細は、support.apple.com/ja-jp/HT212227 および support.apple.com/ja-jp/HT210967 で確認できます。

「探す」ネットワークは、「探す」ネットワーク対応アクセサリプログラムを通じて他社製品（自転車やヘッドフォンなど）にも開放されているため、顧客はiOS 14.3以降およびmacOS 11.1以降で「探す」アプリケーションを使用して、対応する他社製品の位置を特定することができます。

AirTagまたは対応する他社製品を「探す」アプリケーションの「持ち物を探す」に追加するには、Apple IDを持っていること、iCloudアカウントにサインインして「探す」を有効にしていること、そしてAirTagまたは対応する他社製品をそのApple IDに登録することが必要です。その通信はエンドツーエンドで暗号化され、AppleはAirTagまたは対応する他社製品の位置情報を閲覧できません。詳細は、support.apple.com/ja-jp/HT211331 で確認できます。

シリアル番号があれば、Appleは、請求者の国において適切かつ法的に有効な請求に対して、ペアリングされたアカウントの詳細情報を提供できる場合があります。AirTagのペアリング履歴は、最長25日間保持されます。AirTagのシリアル番号の調べ方は、support.apple.com/ja-jp/HT211658 で確認

できます。

Apple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ご注意ください。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」の英字を含むシリアル番号に関する請求には対応できません。法的請求にシリアル番号が5つ以上含まれる場合、Appleは、これらのシリアル番号を編集可能な電子的形式で送信することも求めます（Numbers、Excel、Pages、Wordなどの文書）。

K. パスコードロックされたiOSデバイスからのデータ抽出

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、AppleはiOSデバイスのデータ抽出を実行できません。法執行機関から通常求められるデータは暗号化されており、Appleは暗号鍵を保有していないからです。iPhone 6以降のすべてのデバイスモデルは、iOS 8.0以降のバージョンを搭載しています。

iOS 4からiOS 7までを搭載したデバイスの場合、Appleは、デバイスのステータスによっては、カリフォルニア州の電子通信プライバシー保護法（CalECPA、California Penal Codeのセクション1546～1546.4）に従って、iOSデータの抽出を実行できます。Appleが上述の条件を満たすデバイスのiOSデータを抽出するためには、法執行機関はCalECPAに従い相当な理由に基づく捜査令状を取得する必要があります。CalECPA以外に、法執行機関の捜査に際し、Appleに第三者としてデータを抽出することを請求できるいかなる法的権限もAppleは確認しておりません。

L. IPアドレスの提供請求

IPアドレスを識別子とした法的手続きを提出する前に、Appleは法執行機関に対し、対象のIPアドレスがパブリックIPアドレスまたはルーターのIPアドレスではないこと、およびキャリアグレードネットワークアドレス変換（CGNAT）を使用していないことを確認し、それが非公開IPアドレスであることを法的手続きのサービス提供中にAppleに確証することを求めます。さらに、そのような請求には、3日以内の日付制限を含める必要があります。そのような請求に応じて、Appleは接続ログ（以下のセクションIII.Qを参照）を作成できる場合があります。法執行機関はこのログからAppleアカウント／Apple IDを特定し、それをフォローアップの法的手続きで識別子として使用することを試みることができます。IPアドレスに基づくAppleの顧客データがある場合は、請求者の国において適切かつ法的に有効な請求によってこれを入手できます。

M. 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の識別子です。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。シリアル番号（iOSデバイスの場合はIMEI、MEID、またはUDID）をAppleに提供することにより、対応するMACアドレス情報がある場合は、請求者の国において適切かつ法的に有効な請求によってこれを入手できます。

N. Apple StoreのCCTVデータの提供請求

CCTVデータは、店舗によって異なる場合があります。CCTVデータは通常、Apple Storeで最長30日間保持されます。
多くの法域では現地法に則り、CCTVデータの保持期間は24時間のみです。この期間が経過すると、データは利用できなくなります。CCTVデータのみを請求する場合は、lawenforcement@apple.com宛てにメールを送信してください。政府または法執行機関は、請求するデータの具体的な日付、時間、および関連する取引情報を提供してください。

O. Game Center

Game Centerとは、Appleが提供するソーシャルゲームネットワークです。顧客またはデバイスのGame Centerへの接続に関する情報がある場合があります。接続ログが存在する場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

P. iOSデバイスのアクティベーション

顧客が通信事業者を利用して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、特定の情報が当該事業者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といった情報がある場合があります。こうした情報がある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

デュアルSIM：デュアルSIMに対応しているデバイスについては、nano-SIMまたはeSIMの通信事業者情報がある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。eSIMは、物理的なnano-SIMを使うことなく通信事業者のモバイル通信プランをアクティベートできるデジタルSIMです。詳細は、support.apple.com/ja-jp/HT209044で確認できます。中国本土、香港、マカオの場合、iPhone 12、iPhone 12 Pro、iPhone 12 Pro Max、iPhone 11、iPhone 11 Pro、iPhone 11 Pro Max、iPhone XS Max、iPhone XRは、2枚のnano-SIMカードを使ったデュアルSIMに対応しています。

Q. 接続ログ

Apple Music、Apple TVアプリケーション、Apple Podcast、Apple Books、iCloud、My Apple ID、Appleサポートコミュニティなどの Appleのサービスに対して、顧客またはデバイスから接続があった場合、そのログを Appleから入手できます。IPアドレスを含むこれらの接続ログがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

R. My Apple IDとiForgotのログ

顧客のMy Apple IDとiForgotのログをAppleから入手できる場合があります。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アドレスを含む接続ログがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

S. 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がそのデータを復号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、顧客間においてコミュニケーションが実際になされたことを示すものではありません。FaceTime通話の招待ログは最長25日間保持されます。FaceTime通話の招待ログがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

T. iMessage

iMessageによる通信は、エンドツーエンドで暗号化されます。iMessageのデータがデバイス間で送受信されている間、Appleがそのデータを復号することはできません。iMessageによる通信をAppleが傍受することはできず、AppleはiMessageの通信ログを保持していません。iMessage機能のクエリログは、Appleが保持しています。このログは、デバイスのアプリケーション（メッセージ、連絡先、電話、またはその他のデバイスのアプリケーション）によってクエリが開始されて、検索ハンドル（電話番号、メールアドレス、Apple IDなど）が「iMessage機能に対応」しているかを識別するためにAppleのサーバに送られたことを示します。iMessage機能のクエリログは、顧客間においてコミュニケーションが実際になされたことを示すものではありません。Appleは、iMessageによる通信が実際に行われたかどうかをiMessage機能のクエリログに基づいて判断することはできません。また、クエリを開始した実際のアプリケーションを特定することもできません。iMessage機能のクエリログは、iMessageによる通信が実際に試みられたことを裏付けるものではありません。iMessage機能のクエリログは最長25日間保持されます。iMessage機能のクエリログがある場合、請求者の国において適切かつ法的に有効な請求によって入手できます。

U. Apple TVアプリケーション

Apple TVアプリケーションを使用することで、顧客は、Apple TV+、Apple TVチャンネル、ならびに他社製アプリケーションおよびサービスのテレビ番組や映画について、閲覧、購入、サブスクリプション登録、および再生を行うことができます。購入およびダウンロードの履歴を入手できる場合があります。

Apple TVアプリケーションに関する顧客データを請求する際は、Appleのデバイス識別子（シリアル番号、IMEI、MEID、もしくはGUID）または関連するApple ID／アカウントのメールアドレスを必ず提供してください。Apple ID／アカウントのメールアドレスが不明な場合、対象の顧客アカウントを特定するために、顧客情報を氏名と電話番号、または氏名と住所という組み合わせでAppleに提供する必要があります。政府または法執行機関の担当者は、有効なApple注文番号、またはApple TVアプリケーションでの購入に関連付けられたクレジットカード／デビットカードの完全な番号を提供することもできます。こうしたパラメータと顧客の氏名を組み合わせて提供することもできますが、情報を入手するためには顧客の氏名だけでは不十分です。

注意：法的請求にクレジットカード／デビットカードの完全なデータが含まれる場合、データの安全のため、そのデータはパスワード保護または暗号化された文書（PDF、およびNumbers、Excel、Pages、Wordなどの編集可能な形式の文書）で lawenforcement@apple.com 宛てに送信し、そのパスワードを別のメールで送信してください。また、システムのセキュリティ基準により、Appleが、メールで提供されたリンクから法的請求の文書をダウンロードすることはありません。

V. Appleでサインイン

「Appleでサインイン」は、顧客が自らの既存のApple IDを使用して、プライバシーにより配慮した方法で他社製アプリケーションやウェブサイトにサインインするための仕組みです。対応しているアプリケーションまたはウェブサイト上にある「Appleでサインイン」ボタンを使用することで、顧客は自分のApple IDを使ってアカウントを設定し、サインインできます。ソーシャルメディアのアカウントを使用したり、フォームに入力して別の新しいパスワードを選択したりする代わりに、顧客は、「Appleでサインイン」ボタンをタップするだけで、情報を確認し、Face ID、Touch ID、または自分のデバイスのパスコードを使用して、迅速かつ安全にサインインできます。詳細は、support.apple.com/ja-jp/HT210318 で確認できます。

「メールを非公開」は、「Appleでサインイン」の機能の1つです。この機能は、Appleのプライベートメールリレーサービスを利用して、一意かつランダムなメールアドレスを作成して共有し、顧客の個人用メールアドレスにメールを転送します。基本的な顧客情報は、請求者の国において適切かつ法的に有効な請求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について、Appleにメールで質問することはできますか？
A：はい。政府機関の法的手続きに関する質問またはお問い合わせは、lawenforcement@apple.com 宛てにメールで送信してください。

Q：デバイスを機能させ使用するためにはAppleへの登録が必須ですか？
A：いいえ。デバイスを機能させ使用するためにAppleに登録する必要はありません。

Q：現在ロックされている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は顧客のパスコードにアクセスできません。

Q：紛失されたデバイスまたは盗難にあったデバイスを所有者に返却するためのサポートは得られますか？
A：そのような場合は、lawenforcement@apple.com までお問い合わせください。その際は、デバイスのシリアル番号（または存在する場合はIMEI）とその他関連する情報をメールに記載してください。シリアル番号を確認する方法は、support.apple.com/ja-jp/HT204308 で確認できます。

顧客情報が存在する場合、Appleから顧客に連絡し、デバイスを取り戻す目的で法執行機関に連絡するための詳細情報を提供します。ただし、入手可能な情報から顧客を特定できない場合、有効な法的請求を提出するようにお願いすることがあります。

Q：Appleは紛失されたデバイスまたは盗難にあったデバイスをリストにして管理していますか？
A：いいえ。Appleは紛失されたデバイスまたは盗難にあったデバイスをリストにして管理していません。

Q：法執行機関が捜査を完了した、または刑事事件が解決したあと、Appleが提供した情報はどのように処理する必要がありますか？
A：政府または法執行機関に提供された、個人を特定できる情報を含む情報およびデータ（作成されたすべてのコピーを含む）は、関連する捜査、刑事事件、およびすべての控訴の機会がなくなったあとに必ず破棄してください。

Q：法執行機関から情報提供請求があった場合、Appleは関係する顧客への通知を行いますか？
A：はい。政府、法執行機関、および民間の当事者からアカウントに対する請求があった場合、Appleの通知に関するポリシーが適用されます。Appleは顧客およびアカウント所有者に通知します。ただし、機密保持命令がある場合、適用法により通知が禁止される場合、当該通知によって一般人に深刻

な傷害もしくは死亡の危険がただちに及ぶ可能性があるとAppleが独自の裁量により合理的に判断する場合、児童が危険にさらされる問題と関わる場合、または背景事情を考慮すると通知が適切ではない場合を除きます。