
Lookout, Inc.

**個人向けアプリケーション
プライバシーに関する通知**

発効日:2020 年 1 月 1 日 初版
発行日:2016 年 11 月 15 日
改訂日:2023 年 1 月 1 日

1.	はじめに	3
2.	LOOKOUT が収集する情報	3
A.	情報のカテゴリ	3
B.	LOOKOUT BASIC 個人向けアプリで LOOKOUT が収集する情報	4
C.	LOOKOUT PREMIUM 個人向けアプリで LOOKOUT が収集する情報	5
D.	LOOKOUT PREMIUM PLUS 個人向けアプリで LOOKOUT が収集する情報	5
E.	サードパーティ ソースから LOOKOUT が収集する情報	5
3.	LOOKOUT がお客様の情報を使用する方法	6
4.	LOOKOUT がお客様の情報を開示する方法	7
5.	お客様が選択できること	8
A.	設定へのアクセスと更新	8
B.	メールのオプトアウト	8
6.	データ保持	8
7.	セキュリティ	9
A.	LOOKOUT の責任	9
B.	お客様の責任	9
8.	16 歳未満のユーザー	9
9.	国外のデータ転送	9
10.	カリフォルニア州在住者向けの補足条項	10
A.	個人情報	10
B.	お客様の権利	11
11.	欧州経済地域 (EEA) 居住者向けの補足条項	12
A.	処理の法的根拠	12
B.	PRIVACY SHIELD	12
12.	データ主体の権利	13
13.	質問や懸念がある場合の連絡先	14

1. はじめに

本文書は、当社の個人向けアプリケーションのプライバシーに関する通知 (以下、「本通知」) であり、お客様が Lookout 個人向けアプリケーション (以下、「個人向けアプリ」) を使用する際に当社がお客様から収集する情報と、その情報の使用方法について説明します。個人向けアプリの使用には本通知と Lookout [サービス利用規約](https://www.lookout.com/legal/terms) (www.lookout.com/legal/terms で参照可能) が適用されるため、これら両方をお読みになることが重要です。個人向けアプリの使用以外の方法で Lookout がお客様から収集した情報には、別のプライバシー通知が適用されます。

本通知は、当社の製品とサービス、および Lookout とお客様に適用される法律の変更に対応するために改訂される場合があります。本通知に重大な変更を加えた場合は、お客様に通知いたします。改訂後の通知に記載された方法で個人情報が使用されることを希望しない場合、お客様はアカウントを閉じることが必要になります。

本通知は、Lookout モバイル アプリケーションのログイン画面、Lookout 個人向けアプリの設定、および当社の Web サイトから参照できます。

2. Lookout が収集する情報

Lookout の個人向けアプリ内には複数の層があります。層が上がるごとにさらに多くの Lookout セキュリティ機能にアクセスできます。これらのサービスを提供するために必要な情報はそれぞれ異なる場合があります。お客様から直接収集される情報、お客様の端末から収集される情報、および当社がこの情報をどのように使用するかを理解できるように、本文書に列挙します。iOS および Android デバイス用の個人向けアプリの製品機能の詳細については、<https://www.lookout.com/products/personal/ios> および <https://www.lookout.com/products/personal/android> を参照してください。

- a. **情報のカテゴリ。** Lookout または Lookout のパートナーは、お客様が個人向けアプリを使用中に次のカテゴリの情報を収集することがあります。
 - i. **登録データ:** メールアドレスとパスワードを含みます。
 - ii. **端末データ:** 機器識別情報 (携帯電話番号など)、端末の種類と製造元、オペレーティング システムの種類とバージョン、携帯電話キャリア/事業者、ネットワーク タイプ、発信国、Wi-Fi ネットワーク SSID、インターネット プロトコル (「IP」) アドレス、リクエストの日時などです。
 - iii. **アプリケーション データ:** お客様のモバイル端末にインストールされているすべてのアプリケーションのメタデータを含みます (アプリの名前やバージョンなどが含まれますが、それらに限定されません)。特定の状況では、これまで分析したことのないアプリケーションに遭遇した場合、お客様の端末にあるアプリケーション ファイルの一部または全部のコピーを収集することもあります。このデータは、他のお客様から個人を特定できないようにするために、匿名化され、集計された状態で保持されます。また、アプリケーションがお客様の端末上でどのように動作しているか (たとえば、お客様の電話料金に課金される可能性のあるプレミアムレートの SMS メッセージをアプリケーションが送信しているかどうか)、およびアプリケーションが通信に使用するネットワーク サービスに関する情報を収集する場合もあります。
 - iv. **位置データ。** 当社が提供する機能には、お客様のモバイル端末の位置を特定することでより効果的に動作するものがあります。最初の登録時にお客様の同意を得られた場合、Lookout は次の 2 つの方法で位置情報を収集することがあります。お客様のモバイル端末から直接受信するか、状況によっては、基地局や Wi-Fi ホットスポット情報から位置データを推測します。サードパーティのサービス

個人向けアプリケーションのプライバシーに関する通知

プロバイダーを使用して、その情報を使用可能な位置情報に変換することもあります。モバイル端末の設定で位置情報サービスをオフにすれば、位置情報データが共有されないようにできますが、その場合、Lookout から提供される機能が影響を受ける可能性があります。

- v. **盗難アラート データ**、位置データ、および Theft Alerts 機能が作動したときに撮影された写真が含まれます。
- vi. **支払いデータ**: お客様が Premium および Premium Plus バージョンのアプリケーションを購入した時に、Lookout のパートナーが直接収集した、お客様のクレジットカード番号、有効期限、セキュリティコード、その他の該当する請求情報が含まれます。
- vii. **Web コンテンツ データ**、悪意のあるコンテンツの URL とドメイン、およびそれらの URL が安全でないかどうかを判断するために追加の分析が必要なコンテンツ (URL にフィッシング攻撃やマルウェアが含まれているかどうかなど) が含まれます。閲覧履歴は収集されません。
- viii. **ID 盗難保護データ**: これは、Lookout Premium Plus を購入した場合に提供されるオプションです。個人情報 (運転免許証番号、社会保障番号、パスポート番号、またはその他の ID 番号)、財務情報 (銀行口座、デビットカード番号、クレジットカード番号など)、医療保険番号、および氏名や役職 (またはお客様がサービスに登録している他の人々) といったその他のデータが、Lookout のパートナーである CSIdentity (現在は Experian の一部) によって直接収集される場合があります。
- ix. **分析データ**: Mixpanel、Braze、mParticle などのサードパーティ ツールが含まれます。これらのツールを使って Lookout は、お客様のサービスの利用に関するデータの分析と集計を行います。[MixPanel プライバシー ポリシー](#)、[Braze プライバシー ポリシー](#)、および [mParticle プライバシー ポリシー](#) をお読みになることをお勧めします。

製品の機能は層によって異なるため、Lookout では、以下で詳しく説明するように、お客様が使用している層に基づいて異なる種類の情報を収集する場合があります。

b. Lookout Basic 個人向けアプリで Lookout が収集する情報

- i. **登録データ**。アカウントを作成するには、お客様はメールアドレスとパスワードを提供する必要があります。
- ii. **端末データ**。お客様が Lookout サービスを使用すると、上記の第 2 項 (a) 条 (ii) 号に記載されているように、当社のサーバーはお客様のモバイル端末に関する特定の情報を記録します。
- iii. **アプリケーション データ**。お客様が Lookout サービスを使用すると、上記の第 2 項 (a) 条 (iii) 号に記載されているように、これまで分析したことのないアプリケーションに遭遇した場合、当社はアプリケーションファイルを収集し、お客様の端末にあるアプリケーション ファイルの一部または全部のコピーをダウンロードします。ただし、お客様がそれらのアプリケーションに入力したユーザーデータは収集しません。Lookout は、お客様がモバイル端末上のアプリケーションに入力するユーザー データを収集することはないので、お客様のメールや SMS のメッセージを収集したり、読み取ったり、閲覧したり、スキャンしたりすることはありません。Lookout は、お客様の写真や動画を収集することはありませんが、写真や動画ファイル内に潜む特定の脅威からお客様を保護するために端末上でローカルにそれらのファイルをスキャンすることがあります。
- iv. **位置データ**。有効化されていれば、Lookout の Missing Device 機能 (遠隔操作で端末を Locate and Scream できる) は、位置データを使用します。これは、お客様が携帯電話を紛失しバッテリーが切れてしまった場合でも、最後に端末を認識した場所付近で携帯電話の位置を特定するのに役立ちます。

また、Signal Flare を有効にしている場合、端末のバッテリー残量が少なくなると、この機能が位置データを収集して Lookout に送信します。

c. Lookout Premium 個人向けアプリで Lookout が収集する情報

Lookout は、Lookout Basic 個人向けアプリに記載されている情報と同じ情報を収集します。この情報に加えて、次に説明するように、Lookout のパートナーが、プレミアム機能を提供するためにお客様の支払いデータを直接収集したり、Safe Browsing 機能を使用できるように Web コンテンツ データを収集したり、Theft Alerts 機能を提供するために盗難アラート データを収集したりします。

- i. **支払いデータ。** お客様が Lookout サービスの Premium または Premium Plus サブスクリプションを当社から直接購入した場合、当社はサードパーティの決済処理業者を通じて支払いデータを収集します。サードパーティ ベンダーは、この情報を使用してサービスの請求をお客様に行います。Lookout はお客様の Premium/Premium Plus アカウント (またはその両方) に関する情報を保持します。この情報には、お客様が支払った金額と支払い方法が含まれます。当社はお客様のクレジット カード情報や銀行情報を保持しません。サードパーティの決済処理業者がこの情報を保持します。Lookout アプリを App Store またはご利用のキャリア プランから購入した場合は、お客様の支払い情報は、該当するアプリストアまたはキャリアによって管理されます。支払いに関する情報を Lookout が受け取ることはありません。支払いの処理はいくつかの方法で行うことができます。サービスをお客様に提供できるよう、App Store からお客様の購入の確認通知が Lookout に届きます。キャリアが、お客様の電話番号、加入者 ID、SKU、およびその他の財務関連のものではない情報を共有する場合があります。App Store やご利用のキャリアが、クレジット カードや請求情報のデータを共有することはありません。詳細については、ご利用の App Store またはキャリアの決済処理ポリシーと手続きを参照してください。
- ii. **Web コンテンツ データ。** Safe Browsing サービスを提供するために、Lookout は Web コンテンツ データを使用します。自分が訪問した安全でない URL を記録しないようにする場合は、Safe Browsing をオフにできます。オフにしても、その他のすべての Lookout 機能は引き続き動作します。
- iii. **盗難アラート データ。** Theft Alerts が作動すると、写真が撮影されます。撮影した写真と位置データ (GPS 位置情報) が当社のサーバーに一時的に保存され、その写真と端末の地図上の位置情報を付けたメールがお客様に送信されます。その後画像はサーバーから削除されます。このメールはお客様のアカウントに関連付けられているアドレスに送信されるため、アカウント設定のメールアドレスを最新の状態に保つようにしてください。

d. Lookout Premium Plus 個人向けアプリで Lookout が収集する情報

Lookout は、Lookout Premium 個人向けアプリに記載されている情報と同じ情報を収集しますが、この情報の他に、Lookout のパートナーがお客様から ID 盗難保護データも収集します。

- i. **ID 盗難保護データ。** Identity Theft Protection 機能を使用する時、当社のサードパーティ パートナーである CSIdentity (現在は Experian の一部) が提供する特定の ID 保護監視サービスに登録するため、前述の ID 盗難保護データを入力する場合があります。CSIdentity が収集して保存するお客様に関する情報は、お客様が個人向けアプリ内で入力した情報によって異なります。CSIdentity は、お客様にサービスを提供するために、お客様の ID 盗難保護データをサードパーティのサービス プロバイダー (身元確認会社、消費者報告機関、信用調査会社、支払確認会社、法執行機関など) に伝達する必要がある場合があります。

e. サードパーティ ソースから Lookout が収集する情報

上記のように、Lookout はサードパーティから分析データを受け取ります。

3. Lookout がお客様の情報を使用する方法

当社がお客様の情報を収集するときは、特に明記されていない限り、当社が情報を保管し、その情報をお客様のアカウントに関連付けます。当社がお客様にサービスを提供するには、特定の種類の情報が必要になることをご理解ください。お客様がそうした情報を提供しない場合、または削除することを求められる場合、サービスにアクセスできなくなります。当社は、お客様のプライバシーを非常に真剣に受け止め、本通知に記載されている事業および商業目的にのみ、この情報を使用および開示します。当社によるお客様の情報の使用方法は、以下のようにデータの種類によって異なります。

- a. **アプリケーション データ。** このデータを使用してサービスを提供します。つまり、アプリケーション ファイルのスキャンを実行し、悪意のある動作をしているアプリケーションがないかどうかを判断します。当社はさらにデータを匿名化して情報を集計し、地域ごとのアプリケーションの流行を生み出し、モバイル脅威分析を実施します。このモバイル脅威分析データは、データ プライバシーを確保するために匿名化されます。顧客データを安全かつ機密性の高い方法で集約することにより、Lookout は現在のセキュリティの脅威をより良く把握し、Lookout サービスを向上させることができます。
- b. **端末データ。** 端末の自動スキャンが定期的に実行され、お客様の端末上のアプリケーション、デバイス、オペレーティング システムのファイルに関する詳細情報が収集される場合があります。Lookout は、当社のサービスによって実行されたスキャンの結果と、端末の最新のセキュリティ傾向を収集します。さらに、脅威定義の定期的な更新も実行されます。これらのアクティビティは、個人向けアプリがお客様のモバイル端末上の脅威を検出して対処できるようにすることで、お客様のモバイル エンド ポイントを保護するのに役立ちます。Lookout は、可能な場合にクライアント端末情報を使用して、オペレーティング システムを更新する必要があることをお客様に通知することがあります。お客様が当社に提供した情報と当社が Lookout サービスを提供するためにお客様のモバイル エンドポイント端末から収集した情報以外にも、当社はデータ分析を行うためにお客様の端末から収集した情報を使用します。こうした分析から、製品の機能と使いやすさを向上させるために役立つ重要な情報を得ることができます。モバイル エンドポイント端末でお客様が Lookout アプリケーションを使用する頻度、モバイル エンドポイント端末の Lookout アプリケーション内で発生するイベント、Lookout アプリケーションがモバイルエンドポイント端末上にダウンロードされた場所などの情報を分析します。既知の脅威と新しい脅威の分析を行うために、この情報も集計した状態で使用します。
- c. **ID 盗難保護データ。** CSIdentity がこの情報を使用して、お客様の ID を確認し、リクエストされた ID 保護サービスを提供します。ID 盗難保険が含まれる Premium Plus サブスクリプションにアップグレードすると、Lookout のパートナーがお客様の情報を使用して、お客様の ID が侵害された場合に受けられる支援および適用される保険保障を提供します。
- d. **位置データ。** Lookout の Missing Device 機能には、lookout.com で個人アカウントから遠隔操作で端末を Locate and Scream できる機能が含まれており、お客様が携帯電話を紛失しバッテリーが切れてしまった場合でも、最後に端末を認識した場所付近で携帯電話の位置を特定するのに役立ちます。Signal Flare を有効にしている場合、端末のバッテリー残量が少なくなると、この機能が位置データを収集して Lookout に送信します。Lookout がバッテリー残量低下アラートを受信すると、携帯電話の位置が lookout.com に保存されます。この機能は、個人アプリの設定でオン/オフを切り替えることができます。
- e. **登録データ。** 当社は、お客様のメールアドレスを使用して、Lookout またはビジネス パートナーから製品のお知らせや特別なプロモーションに関する情報をお客様に送信する場合があります。お客様がサポートを受けるために Lookout にメールを送信した場合、当社はお客様へのサポート提供および

サービス向上のために、その情報を保持することがあります。当社は、お客様のメールアドレスを使用して、お客様の端末とサービスに関する連絡を行う場合があります、それにはプライバシーまたはセキュリティ関連の通知の送信や Lookout サービスの重要な変更の通達などが含まれます。

- f. **盗難アラート データ。**当社はこの情報を使用して、盗難アラート サービスを実行します。
- g. **Web コンテンツ データ。**Safe Browsing は、安全でない URL を識別して警告し、お客様がそのような URL の読み込みを回避できるようにする機能です。訪問した URL は匿名化され、セキュリティスキャンを実行するために Lookout に送信されます。お客様が訪問する安全でない URL の記録を使用して、お客様がアクセスしようとした URL が安全でないことをお知らせします。

4. Lookout がお客様の情報を開示する方法

本項では、Lookout がどのようにお客様の情報を共有および開示する場合があるかについて説明します。

- a. **サードパーティのサービス プロバイダーとパートナー。**当社は、お客様の製品またはサービスへのリクエストに応えるため、当社の製品およびサービスのサポートを提供するため、製品パフォーマンスのデータを分析するため、および製品を改善するために、お客様の情報を知る必要がある、当社のソフトウェアに統合された製品とサービスを提供するサードパーティ サービス プロバイダーと、お客様の情報を共有する場合があります。例えば、次のような場合です。
 - i. **Identity Theft Protection** サービスをご利用になる場合、お客様に当該サービスを提供するため、お客様の情報が当社のパートナーである CSIdentity (現在は Experian の一部) によって収集されます。さらに CSIdentity は、リクエストされたサービスをお客様に提供するために、お客様のデータをサードパーティのサービス プロバイダー (身元確認会社、消費者報告機関、信用調査会社、支払確認会社、法執行機関など) に提供する場合があります。CSIdentity は、Identity Protection サービスを提供する目的で、モニタリングおよびアラートをお客様に提供したり、お客様 (もしくはお客様が登録した他者) に関する情報およびレポートを取得したりする場合があります。これには、住所履歴、氏名、別名、およびその他のレポートが含まれます。Lookout は、CSIdentity とそのサービス プロバイダーが、Lookout アプリ Premium Plus 製品を通じてサービスを提供する目的でのみ、お客様から収集したデータを使用することを義務付けています。
 - ii. Lookout は、お客様の購入および関連するサポート サービスを適切に提供し、事業に関連する機能を実行するために、お客様の情報を当社の再販業者またはその他の携帯電話事業者と共有する場合があります。
 - iii. Lookout はお客様の情報を使用して、市場調査を実施したり、Lookout の製品やサービスに付加価値を付けられる製品を提供している企業 (携帯電話事業者など) と共同でプロモーション活動を行ったりする場合があります。
- b. **サードパーティの支払いパートナー。**当社は、サービス プロバイダーがお客様から直接情報を収集して、会計、監査、請求の調整、および収集を行うことを許可する場合があります。
- c. **法令遵守。**当社は、以下の目的のために、法律に沿ってお客様の情報を開示することがあります: (i) 法律、規制、または法的プロセス (国家安全保障または法執行要件を満たすことを含む) を遵守する。(ii) 個人、法人、施設の安全またはセキュリティを保護する。(iii) 本通知に対する潜在的な違反に対処する。(iv) 詐欺、セキュリティ、または技術的な問題を調査する。または (v) Lookout またはサードパーティの権利や財産、当社の従業員、ユーザー、および公衆を保護する。当社は、お客様の情報を開示することが法律によって要求されているかどうかを知る権利をお客様が有していると強く信じて

います。そのため、法執行機関からの要請 (召喚状や裁判所命令など) に応じてお客様の情報を開示する前に、お客様のアカウントに記載されているメールアドレス宛てに通知します。ただし、(a) そうすることを当社が禁止されている場合、または (b) 通知することによって負傷や死亡の危険が生じる可能性のある緊急事態の場合、または未成年者に危害が及ぶ可能性のある場合は、この限りではありません。さらに、本通知のいかなる内容も、お客様の情報を開示するようにとのサードパーティ (政府を含む) による要求に対する、お客様による法的な防御や異議を制限することを意図するものではありません。

- d. **Lookout の事業に変化が生じるとき。** 当社の事業の特定部分の実際の買収または買収の提案、合併または買収に関連して、当社はお客様情報を実際のバイヤーまたは見込みバイヤー (およびその代理人とアドバイザー) に対して開示することもあります。ただし、本通知に開示されている目的にのみ情報を使用しなければならないことをバイヤーに通知するものとします。
- e. **匿名化され集計されたデータ。** データ分析には、当社はお客様のデータの一部を含む可能性のあるデータを匿名化し、集約し、要約します。他の人がモバイルの脅威を理解し、特定のモバイル アプリケーションの動作に関する知見を得られるようにするため、このデータ分析の結果として得られたレポートを一般に共有することがあります。
- f. **同意のもとに。** お客様が同意した場合、当社はお客様の情報をサードパーティに開示することもあります。

5. お客様が選択できること

a. 設定へのアクセスと更新

Lookout アカウントの設定は、モバイル アプリの [設定] ページから更新するか、または当社の Web サイト <https://my.lookout.com/user/login> からログインして、Lookout と共有するデータに影響する特定の設定を変更できます。お客様のプライバシーとセキュリティを保護するため、お客様にアカウントへのアクセス権を付与したり、お客様がアカウントに変更を加えたりする前に、お客様の ID を確認するためユーザー名とパスワードの入力を要求します。

b. メールのオプトアウト

各メールにある購読解除リンクを使用して、Lookout からのプロモーション情報の受信をオプトアウトすることができます。オプトアウトのリクエストは通常すぐに処理されますが、削除のリクエストの処理には 10 営業日を見込んでください。当社からのプロモーション メッセージの受信をオプトアウトした後も、Lookout サービスに関する取引や製品関連のメッセージは引き続き配信されます。アカウント設定で、これらの通知メッセージの一部をオプトアウトすることができます。

6. データ保持

Lookout は、当社の製品とサービスをお客様に提供するために合理的に必要である場合、もしくは法令遵守の目的上必要である場合に限り、個人データ (この用語の定義は GDPR に従います) を含むお客様の情報を保持するものとしています。

7. セキュリティ

a. Lookout の責任

Lookout はセキュリティ企業であり、お客様のデータを保護することは当社にとって重要です。Lookout は、商業上合理性のある物理上、管理上、技術上の保護手段を使用して、お客様情報を処理することのリスクに見合った技術的および組織的な措置を確実に講じています。たとえば、ファイアウォール、認証、物理的なセキュリティ、その他の保護手段を組み合わせ、お客様のアカウントとお客様のデータを保護しています。お客様が Lookout アプリ内で機密情報 (位置データなど) を入力すると、その情報は転送中にも格納時にも **Secure Socket Layer 技術 (SSL)** を使用して暗号化されます。また、サードパーティの侵入テストを実行して、攻撃に耐えるよう当社システムを強化しています。Lookout は、複雑な技術的脅威やその他の犯罪の脅威から保護するための制御を実装し、不注意な従業員からも保護するために、あらゆる適正な努力を払っています。

100% 安全といえるインターネット上の送信手段や電子的保存方法は存在しないため、Lookout サービスを運用するために当社がお客様の代わりに受信する、またはお客様が Lookout に伝送する情報、データ、コンテンツのセキュリティを保証することはできません。お客様の情報の受信や送信はすべて、お客様ご自身の意思に基づき、お客様ご自身の責任において行われます。当社の物理的、技術的、管理上の保護手段を突破して、そのような情報がアクセス、開示、変更、破壊されることは絶対には保証できません。

お客様に影響を与える可能性のあるセキュリティ侵害が検出された場合、当社はお客様に電子的に通知して、適切な保護措置を講じることができるようにします。セキュリティ侵害が発生した場合、Lookout は Lookout サービスにも通知を投稿します。お住いの地域によっては、お客様がセキュリティ侵害の通知を書面で受け取る法的権利を保有している場合があります。

b. お客様の責任

パスワードを他者に知られないように常に管理することは、お客様の責任です。他のサービスで使用していない強力なパスワードを使用することをお勧めします。パスワードが漏洩したと思われる場合は、Lookout の Web サイトでパスワードを直ちに変更するか、support@lookout.com までご連絡ください。アカウントに関連付けられているメールアドレスが正確であるようにするのも、お客様の責任です。当社はこの電子メールを使用して、サービスの更新、ポリシーの変更、およびお客様の情報のリクエストや端末で行われた試行の確認といったアカウント活動についてお客様に連絡します。Lookout は、ユーザーが誤ったメールアドレスを指定した結果としてサードパーティに送信された情報については責任を負いません。

8. 16 歳未満のユーザー

Lookout は、提供するサービスがその子供の親の購入した複数端末プランに含まれており、Lookout サービス利用規約に記載されている収集と保管に親が同意している場合を除き、16 歳未満の子供に関する個人データを故意に収集または保存することはありません。お子様が親の同意なしにこのサービスを利用していると思われる場合は、privacy@lookout.com までご連絡ください。

9. 国外のデータ転送

Lookout は、サンフランシスコに拠点をもち、サーバーは米国に配置されています。米国外のユーザーから収集された個人情報は、米国に送られます。米国外で Lookout サービスを使用しているお客様の情報は、

サーバーが設置され、データベースが運用されている米国に転送され、そこで保存、処理されることがあります。

10. カリフォルニア州在住者向けの補足条項

a. 個人情報

カリフォルニア州消費者プライバシー法 (以下、「CCPA」) およびカリフォルニア州プライバシー権法による CCPA の改正に従い、Lookout が個人向けアプリを通じて、またはその他の方法で収集する個人情報 (この用語の定義は CCPA に従います) のカテゴリ、個人情報を収集する情報源のカテゴリ、個人情報を収集する事業上の目的、個人情報を共有するサードパーティのカテゴリは以下のとおりです。下の表に記載の情報は、過去 12 か月間の実績に基づきます。

個人向けアプリケーションのプライバシーに関する通知

個人情報のカテゴリ	情報源のカテゴリ	事業上の目的	Lookout が事業目的で個人情報を販売、共有、または開示する組織のカテゴリ
メールアドレス、IP アドレス、Wifi SSID などの端末識別情報を含む識別情報	消費者	サービスの提供、サービスの改善、カスタマーサービス、分析	データ分析サービスプロバイダー、サービスプロバイダー、下請業者
*SSN、運転免許証番号、クレジットカード番号、銀行口座番号を含む ID 盗難保護のための識別情報	消費者	サービスの提供	サービスプロバイダーおよび下請業者
位置データ	消費者	サービスの提供	サービスプロバイダーおよび下請業者
消費者によるウェブサイトまたはアプリケーションの利用状況に関する情報	消費者	サービスの提供	サービスプロバイダーおよび下請業者

*ID 盗難保護のための識別情報はすべて、消費者が直接入力し、Lookout のサービスプロバイダーである CSID (現在は Experian の一部) が保管し、サービスの提供のみを目的として使用されます。

b. お客様の権利

CCPA に従い、例外に従うことを条件に、カリフォルニア州の消費者 (この用語の定義は CCPA に従います) は以下の権利を有します。

- i. **アクセス。** お客様は、Lookout が収集したお客様の個人情報のカテゴリ、または Lookout が収集したお客様の特定の個人情報を、開示および提供するよう Lookout に求める権利を有します。
- ii. **削除。** お客様は、法律に定められる一部の例外に従うことを条件に、特定の状況において、自身の個人情報の削除を求める権利を有します。
- iii. **修正。** お客様は、Lookout が保存している個人情報を修正または変更する権利を有します。
- iv. **差別の禁止。** お客様は差別されない権利を有します。これには、本条のいずれの権利であれ、それを行なったことを理由に、サービスに対して異なる料金を請求されたり、サービスの利用を拒否されたりしない権利が含まれますが、それに限定されません。また Lookout は、CCPA が定めるいかなる権利をお客様が行使した場合にも、お客様を差別しません。
- v. **オプトアウト。** Lookout は Lookout 個人向けアプリのユーザーの個人情報を販売することも、共有することもないため、この権利はカリフォルニア州にお住まいのお客様には適用されません。
- vi. **要配慮個人情報の使用の制限。** Lookout は、CCPA 規制の第 7027 条 (m) 項で許可された以外のいかなる目的でも、お客様の「要配慮個人情報」 (この用語の定義は CCPA に従います) を処理しないため、この権利はカリフォルニア州にお住まいのお客様には適用されません。

お客様は、(1) <https://personal.support.lookout.com> からアクセスできるウェブフォームに入力するか、(2) Privacy@Lookout.com 宛てに要請を送信するか、いずれかの方法により、ご自身の情報にアクセスする、またはご自身の情報を削除する権利を行使できます。上記第 5 条 (a) 項に記載のとおり、お客様のプライバシーとセキュリティを保護するため、お客様の個人情報へのアクセスまたは削除の要請を許可するにあたっては、本人確認のためユーザー名とパスワードを使ってお客様にアカウントにログインしていただく必要があります。本人確認ができない場合は、アクセス要請に対して具体的な個人情報は一切開示しません。また、削除要請に対しては、個人情報の削除要請を却下するものとします。個人情報の削除

要請については、2段階のプロセスで対応するものとします。お客様はまず、明確な削除要請を送信し、次に個人情報の削除を希望する旨を別途確認する必要があります。カリフォルニア州の消費者であるお客様は、ご本人に代わって委任代理人がアクセスまたは削除の要請を行うことができます。ただし、委任代理人がお客様からの書面による許可を受けていること、およびお客様が直接 Lookout で本人確認を行えることが条件となります。

11. 欧州経済地域 (EEA) 居住者向けの補足条項

a. 処理の法的根拠

お客様が EEA からアクセスしている場合、Lookout がお客様の個人データ (この用語の定義は一般データ保護規則 (以下、「GDPR」) に従います) のデータ管理者になります。本通知に記載されているようにお客様の個人データを収集および使用する法的根拠は、関係する個人データおよび当社がそのデータを収集する具体的なコンテキストによって異なります。ただし、当社がお客様から個人データを収集するのは、通常次の場合に限られます: (a) お客様の個人情報の使用が、お客様との契約に基づく当社の義務を履行するために (たとえば、お客様が Lookout アプリをダウンロードし使用することで同意したサービス規約を遵守するために) 必要である、または (b) お客様の個人情報の使用が、Lookout の正当な利益や他者の正当な利益のために必要である (たとえば、Lookout サービスのセキュリティを確保する、Lookout サービスの運営またマーケティングをする、Lookout の人員または他者の安全な環境を確保する、支払いをする/支払いを受領する、不正を防止する、Lookout サービスの提供先であるお客様について理解するなど)、または (c) お客様の同意を得ている場合 (特定の当社マーケティング活動のためなど)。一部の処理は、適用法を遵守するために行われます。

b. Privacy Shield

Lookout は、EU 加盟国、英国、およびスイスからの個人データの収集、利用、保持に関して、米国商務省が定める [E.U.-U.S. Privacy Shield](#) および [Swiss-U.S. Privacy Shield](#) フレームワークで自己認証しています。これらのフレームワークは、企業が個人データを EU 諸国、英国、およびスイスから米国に転送する際にデータ保護要件を遵守できるように策定されたものです。Privacy Shield に関する詳細情報、および現在 Privacy Shield の下で認証を受けている企業の一覧については、<http://www.privacyshield.gov> をご覧ください。

これらの原則に基づいて必要とされることに従い、Lookout は Privacy Shield の下に置かれた情報を受け取り、Lookout の代理機関としての役割を果たすサードパーティのサービス プロバイダーにその情報を転送する際に、(i) 代理機関が Privacy Shield に反する方法で情報を処理している場合、かつ (ii) Lookout が損害を発生させる事象に対する責任を負っている場合、Lookout は Privacy Shield の下で一定の法的責任を負います。

Privacy Shield Framework に従って受信または転送された個人情報に関して、Lookout は米国連邦取引委員会の規制執行権限の対象となっています。特定の状況において、当社は、国家安全保障または法執行機関による要求を満たすため、公的機関による合法的な要請に応じて個人情報を開示することを要求される場合があります。

当社のプライバシー慣行に関するお客様の懸念に対する Lookout の対応、および Lookout による Privacy Shield に準拠した個人情報の処理方法に不満をお持ちのお客様は、Lookout が指定する Privacy Shield 独立償還請求機構から、無料で支援を受けることができます。詳しい情報については、

<https://www.jamsadr.com/eu-us-privacy-shield> をご覧ください。お客様は、関連する監督機関に苦情を申し立てる権利も保有します。しかし、まず Lookout にご連絡いただければ幸いです。Lookout はお客様の懸念を解決するため、最善を尽くします。お客様は、未解決の苦情の調停も選択できますが、調停を開始する前に、以下を行う必要があります。(1) Lookout にご連絡いただき、当社に問題を解決する機会を与える。(2) 上記の Lookout 指定の独立請願制度の支援を求める。および、(3) 米国商務省に連絡し(直接か、または欧州データ保護局を通じて)、米国商務省に問題の解決に取り組む猶予を与える。Privacy Shield の法的拘束力のある調停手続きについて詳しくは、<https://www.privacyshield.gov/article?id=ANNEX-I-introduction> をご覧ください。各当事者は、自身の訴訟費用を負担する責任を負うものとします。調停者は、Privacy Shield に従って、個人に関する Privacy Shield Principles の違反を解決するのに必要な、個人に固有の、非金銭的かつ公平な救済を課すことのみ可能である点をご了承ください。Lookout は、米国連邦取引委員会 (FTC) の調査執行権限の対象です。

Lookout は、欧州連合司法裁判所 (CJEU) により、Privacy Shield が EU プライバシー法遵守の証明として無効とされていることを認識しています。この枠組みとは独立して、Lookout は常にプライバシーポリシーを通じて、パートナー、お客様、および当社ウェブサイトのご利用者様に対する義務を管理してきました。今後も引き続き、適用される法律、規制、およびその他の行政権限による要求に従い、個人情報保護のための所定の要件を満たすよう取り組んでまいります。さらに Lookout は、EU およびスイスから移転されるデータに関する Privacy Shield の未解決の苦情について、EU データ保護機関 (DPA) とスイス連邦データ保護情報コミッショナー (FDPIC) により設立されたパネルとの協力を努めてまいります。今後も引き続き EU-米国データ プライバシー フレームワーク関連の進展を注視し、常に適用法に従って個人情報を取り扱います。

12. データ主体の権利

英国、EEA、またはデータ保護に関する適用法が定められたその他の法域 (バージニア州、コロラド州、コネチカット州、ユタ州など) の居住者であるお客様は、個人データに関して一定の権利を有する場合があります。これらの権利は、所定の条件により適用が除外される場合があります。これには以下のような権利が含まれます。

- i. **アクセス。**お客様は、当社が処理するお客様の個人データのコピーを要請する権利を有する場合があります。追加のコピーが必要な場合、当社は相応の料金を請求することがあります。
- ii. **修正。**お客様は、当社が保持するお客様の個人データについて、不完全または不正確であるにかかわらず、誤りの修正を要請する権利を有する場合があります。
- iii. **削除。**お客様は、特定の状況 (当社が必要としなくなった、あるいはお客様が同意を撤回した、など) において、お客様の個人データの削除を要請する権利を有する場合があります。「設定へのアクセスと更新」という見出しの上記セクションに基づいて付与されている権利に加えて、ほかにご要望があれば privacy@lookout.com までご連絡ください。
- iv. **ポータビリティ。**お客様は、当社に提供した個人データを、一般的に使用される構造化された機械可読形式で受け取る権利を有します。また、特定の状況においてそのデータをサードパーティに送信する権利を有します。
- v. **異議申し立て。**お客様は、(i) ダイレクトマーケティングを目的とするお客様の個人データの処理に対していつでも異議を申し立てる権利、および (ii) 当社やサードパーティが追求する正当な利益のためにお客様の個人データの処理の法的根拠が必要な場合、係る処理に対して異議を申し立てる権利を有する場合があります。

- vi. **制限。**お客様は、特定の状況 (個人情報の正確性に異議を唱える場合など) において、お客様の個人データの当社による処理を制限するよう要請する権利を有します。
- vii. **同意の撤回。**個人データの処理に関してお客様の同意が必要な場合、お客様はいつでもその同意を撤回する権利を有します。
- viii. **データ監督機関への苦情申し立て。**お住いの法域によっては、お客様は Lookout がデータ保護に関する適用法に違反していると判断した場合、地域のデータ監督機関に苦情申し立てを行う権利を有する場合があります。

これらの権利のいずれかを行使する場合は、privacy@lookout.com までご連絡ください。Lookout は、適用法によって義務付けられた期間内に、お客様からの要請に対応いたします。お客様からの要請に応じるにあたって、まず本人確認をさせていただく場合があります。本人確認は、アカウントに関連付けられたメールアドレスにメールを送信するか、アカウントに関連付けられたその他の情報の提示を求めるという方法で行います。お客様は、委任代理人を指名し、委任代理人がご本人に代わって要請を提出することもできます (ただし、その場合でも本人確認が必要になる場合があります)。

13. 質問や懸念がある場合の連絡先

本通知に関してご意見やご質問がある場合は、Lookout のデータ保護責任者 (宛先: privacy@lookout.com) に問い合わせるか、Lookout, Inc. の次の宛先に郵送してください。宛名: Michael Musi, Data Protection Officer、住所: 3 Center Plaza, Suite 330, Boston, MA (USA) 02108。EEA にお住いのお客様は次の宛先に問い合わせ状を送ることもできます。宛名: Mr. Wim Van Campen, VP, Sales EMEA、住所: Florapark 3, 2012 HK Haarlem, Netherlands。