Mobile Endpoint Security のプライバシーに関する方針

発効日:2016 年 10 月 24 日
公開日:2016 年 10 月 24 日
改訂日:2019 年 4 月 3 日
バージョン:3.0
ステータス:承認済み

Mobile Endpoint Security のプライバシーに関する方針

Lookout は、お客様のプライバシーはセキュリティ同様に重要であると確信しており、当社が収集するデータに関して完全に透明性を保つことで、端末のセキュリティに加え従業員のセキュリティを保護する助けになりたいと考えています。お客様が Mobile Endpoint Sscurity 製品の Privacy Control 機能を MDM プロバイダーと共に使用する際に、Lookout がお客様のユーザー名やメールアドレスなどの個人情報を収集することはありません。Lookout, Inc. (以下「Lookout」または「当社」) は、お客様とお客様の従業員に本 Mobile Endpoint Security のプライバシーに関する方針を提供し、当社の Mobile Endpoint Security 製品 (以下「Mobile Endpoint Security 製品」) に関する情報の取り扱いを説明しています。この Mobile Endpoint Security のプライバシーに関する方針は、お客様がモバイル端末に Mobile Endpoint Security 製品をインストールおよび有効化することに伴い、お客様から収集するデータやお客様に関するデータに適用されます。Mobile Endpoint Security 製品をダウンロードして有効化することで、本 Mobile Endpoint Security のプライバシーに関する方針で説明されるデータの収集、使用、開示および保存の慣行を許可するものとします。

(1) すべてまたは一部の従業員が Mobile Endpoint Security 製品をインストールすることを必要とする、または (2) すべてまたは一部の従業員が Mobile Endpoint Security 製品を含むデバイス管理スイート (MDM) をインストールすることを必要とする企業に雇用された結果として、Mobile Endpoint Security 製品のダウンロードおよびインストールが指示されることがあります。本 Mobile Enterprise Security のプライバシーに関する方針は、Lookout の Mobile Endpoint Security 製品に関する情報の取り扱いのみに適用されることにご注意ください。お客様の雇用主 (以下「雇用主」) またはモバイル端末管理プロバイダー (以下「MDM プロバイダー」) によるデータの収集、使用、開示、およびセキュリティに関する慣行、あるいは Lookout が雇用主に代わって収集するデータについて、ご質問やご要望がおありでしたら、これらの関係者宛にお送りください。

Lookout は、法律、Lookout によるデータの収集および使用に関する慣行、Mobile Endpoint Security 製品の機能、またはテクノロジーの進化を反映して、いつでも本 Mobile Endpoint Security のプライバシーに関する方針を変更する権利を留保します。本 Mobile Endpoint Security のプライバシーに関する方針の変更が公開された後も、引き続き Mobile Endpoint Security 製品を使用された場合は、当該変更に同意したものと見なされます。本プライバシーに関する方針に重大な変更を加える場合は、お客様に通知いたします。

Lookout では、本 Mobile Endpoint Security のプライバシーに関する方針が、Mobile Endpoint Security 製品に対するお客様からの質問に答える構成となるべく努めて参ります。本プライバシーに関する方針には、次のような質問に対する答えが含まれています。

1. Lookout Mobile Endpoint Security 製品とは何ですか?

Lookout Mobile Endpoint Security (MES) とは、モバイル端末を通してアクセスする保護されていないデータのリスクを緩和するモバイル セキュリティ ソリューションです。Mobile Endpoint Security 製品は、アプリ、端末、ネットワーク、ウェブサイトに対するモバイルの脅威を可視化します。Mobile Endpoint Security 製品は、既存のモバイルへの投資とシームレスに統合し、機能を許可する一方で、ヘルプデスクのチケットを最小限に抑えます。1 億 5 千万を超えるセンサーから成るグローバル センサー ネットワークを活用する Lookout MES プラットフォームは、人工知能を駆使して予測型セキュリティを提供し、人の目では捉えられないリスク パターンを示す複雑なパターンを特定します。脅威が検出されると、Lookout から従業員および管理者に解決のオプション (アプリのアンインストール、条件付きアクセスの起動など) が示されます。このソリューションは、通常 Lookout MES を大手 MDM プロバイダーやアイデンティティ プロバイダーと統合することで提供されます。

2. Lookout は、モバイル端末からどのようなデータを収集しますか?

Lookout がサービスを提供するには、特定の種類の情報が必要です。そうした情報をご提供いただけない場合、または削除を求められる場合、Lookout サービスにアクセスできなくなります。

Lookout では、セキュリティ リスクからモバイル端末と従業員を保護するため、サービスを提供するにあたって、端末から特定の種類のデータを収集します。次のようなデータが収集される**可能性があります**。

- モバイル端末のメーカーとモデル
- 画面サイズやファームウェア バージョンなど、モバイル端末の特定の技術的設定
- (国や地理位置情報を特定可能な) IP アドレス
- モバイル端末のオペレーティング システムの種類とバージョン
- モバイル端末固有の端末 ID
- 端末の設定データ：端末がルート アクセスを許可するように設定されているかどうかや、端末のハードウェアの制限が解除されているかどうかなど
- 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 (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)
- モバイル端末の接続先ネットワークに関するメタデータ (ネットワークの SSID やネットワーク機器に固有の MAC/BSSID アドレスなどが含まれますが、それらに限定されません)

- 特定の状況下では、アプリケーションのコピーを収集することもあります
- 端末の製品性能を分析するために使用される追跡ツールからのデータ
- 特定のアプリケーションがセキュリティ上の脅威を与える可能性があるという Lookout からのアラートにどう対応するか
- 端末に Safe Browsing が設定されている場合、サイトが安全かどうかを判断することだけを目的に、お客様が訪問するウェブサイトに関する匿名情報を収集する場合があります

お客様が Mobile Endpoint Sscurity 製品の Privacy Control 機能を MDM プロバイダーと共に使用する際に、Lookout がお客様のユーザー名やメールアドレスなどの個人情報を収集することはありません。

3. Lookout が端末にインストールされたアプリケーションに関する情報を収集するということは、Lookout がメールを読んだり写真を見たりするということですか?

いいえ。Lookout は、お客様がこれら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ありません。Lookout は、端末上のアプリケーションや、アプリケーション自体に関するメタデータのみを収集します。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、メッセージ、写真、動画を収集したり、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。

4. Lookout はモバイル端末以外の場所にある端末の持ち主に関するデータを収集しますか?

Lookout の Mobile Endpoint Security 製品は、MDM プロバイダーと統合せずにインストールされている場合、すべての従業員のモバイル端末が特定のメールアドレスと関連付けられていることを必要とします。そのため、お客様の雇用主は Lookout にお客様のメールアドレスを提供して、MES サービスを有効化することができます。Lookout Endpoint Security 製品が MDM ソリューションと統合され、Privacy Control がオンになっている場合、Lookout がお客様のメールアドレスを収集することはありません。

Mobile Endpoint Security 製品を MDM プロバイダー製品の一部としてインストールした場合、当該 MDM プロバイダーからお客様に関する情報を収集することもあります。プロバイダーのプライバシー慣行については、当該 MDM プロバイダーにお問い合わせください。

Lookout は、お客様に関するその他の情報が、お客様が直接当社に連絡して自らの意思によって開示された場合、あるいは Lookout のパートナーやマーケティング業者等の第三者に提供された場合に、

そのような情報を収集することがあります。Lookout では、この情報を使用して、Lookout およびその製品やサービスに関する最新情報をお客様に提供することがあります。また、Lookout が参加または主催する会議その他のイベントにお客様を招待することもあります。

5. Lookout は、どのタイミングでモバイル端末からデータを収集しますか?

上述の通り、Lookout は Mobile Endpoint Security 製品が MDM なしでインストールされている場合に、お客様の雇用主からメールアドレスを収集します。Mobile Endpoint Security 製品が MDM ソリューションと一緒にインストールされ、Privacy Controls がオンになっている場合、Lookout はメールアドレスを収集しません。Mobile Endpoint Security 製品をダウンロード、インストールまた起動すると、Lookout はすぐに端末からデータの収集を開始します。モバイル端末上にアプリケーションをインストールする、またはそのアプリケーションにアクセスするとき、当社は潜在的なセキュリティ上の脅威を確認するためアプリケーションをスキャンします。

6. Lookout は、モバイル機器から収集したデータをどのように使用しますか?

本 Mobile Endpoint Security のプライバシーに関する方針に従ってお客様の情報を使用する法的根拠は、お客様と雇用主との関係、ならびに雇用主の使用事例に基づいて決まり、次の内容が含まれる場合があります。(a) お客様との契約に基づく Lookout の義務 (お客様の雇用主が雇用契約を履行する、あるいはお客様が Lookout アプリのダウンロードまた使用を通して受諾したサービス規約を Lookout が遵守するなど) を遂行するために必要な個人情報の使用、または (b) お客様の情報の使用が契約の遂行に必要ではないが、Lookout の正当な利益や、雇用主または他者の正当な利益 (Lookout サービスのセキュリティを確保する、Lookout サービスを操作する、Lookout および雇用主のスタッフまたは他者の安全な環境を確保する、支払をする/支払を受領する、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) のために必要な場合、および適切なデータ セキュリティを必要とする法的要件に準拠するために必要な場合。

Lookout は、お客様のモバイル端末から収集したデータを使用することで、お客様やお客様の雇用主に対する脅威を検知したり、Mobile Endpoint Security 製品を改善したり、他の製品提供を改善したりできます。Lookout では、モバイル端末上のアプリケーションを分析するときに、これまで分析したことのないアプリケーションを検出した場合、そのアプリケーションの一部またはすべてのコピーをダウンロードして、リスクをもたらすかどうかを分析また判断する場合があります。Lookout はお客様に、セキュリティ リスクを伴うアプリケーションをアンインストールするか、リスクを無視するかのオプションを提案します。Lookout ではさらに、悪意あるファイルやアプリケーションに対してお客様が取った解決策 (アンインストールや無視など) も収集し、収集したデータを端末のリスクの脅威を分類するために使用することがあります。このデータはメタデータであり、個人データは含まれ

ないため、お客様を特定することはできません。

企業向け製品である Mobile Endpoint Security 製品は、データを収集することで、お客様のモバイル端末のみならず、雇用主のセキュリティも保護します。

お客様のモバイル端末から収集したデータと、第三者から収集したデータを組み合わせて、Mobile Endpoint Security 製品を含む Lookout の製品を改善する場合もあります。このデータは、匿名化されます。分析の結果が公に共有される場合は、全体的に匿名化することで、お客様ならびに雇用主のプライバシーを保護します。

Lookout のデータ処理がお客様の同意に基づいて行われる場合、いつでも同意を取り消すことができますが、同意を取り消すことによって、取り消す以前に行われた処理の合法性に影響を与えることはありません。同意を取り消す方法については、雇用主にお問い合わせください (または該当する場合には、Lookout の以下の連絡先までお問い合わせください)。

7. Lookout はデータを他者と共有しますか?

はい。企業向け製品として、特定のデータがお客様の雇用主と共有されることや、雇用主の許可を受けた人物による閲覧を受けることがあります。Lookout がお客様のデータを広告業者と共有したり、広告業者に販売したりすることはありません。雇用主または雇用主の許可を受けた人物は、Mobile Endpoint Security 製品のダッシュボードを使用して、お客様のモバイル端末のセキュリティに関連する特定の情報に対するアクセス権を付与されます。雇用主は、端末のモデルやキャリアなど、固有の端末属性を見ることができます。雇用主は、Lookout が悪意があると特定したアプリケーションや、雇用主の該当する会社の方針に違反するアプリケーションを把握することができます。該当する会社の方針への違反がお客様に与える影響については、雇用主にお問い合わせください。

Mobile Endpoint Security 製品を MDM プロバイダーの製品の一部としてインストール I および有効化した場合、お客様のモバイル端末から収集したデータを、当該 MDM プロバイダーと共有する場合があります。

Lookout は、お客様に関するデータを、Lookout の系列会社および Lookout の代理としてビジネス関連機能を実行する契約を結んだサービス プロバイダーやパートナーなどの第三者と共有する場合があります。以下を行うサービス プロバイダーなどがこれに該当します。(a) 顧客、技術、または運用上のサポートを提供する、(b) 注文や、ユーザーまたは雇用主のリクエストを実行する、(c) 支払いを処理する、(d) Lookout のオンライン サービスをホスティングする、(e) データベースを維持する、(f) 製品の改善や強化を目的としてデータを分析する、(g) Lookout の Mobile Endpoint Security 製品または他の Lookout 製品とサービスをサポートまたは販売する。Lookout は、召喚状や裁判所命令など Lookout が受領したあらゆる法的手続に対処するため、Lookout の法的権利を確立または行使するため、あるいは法的要求に対して防御するために、お客様に関するデータを開示する場合があります。Lookout は、地方、州、連邦、または外国の法執行機関から情報提供要請を受けた場合、雇用主に当該要請を

転送し、処理していただくよう努めますが、そうした対処が法的に適切であると見なした場合は直接対応し、要請された情報を提供する権利を留保します。Lookout は、違法行為や不正が疑われる場合、いずれかの人物の物理的安全に対する脅威となり得る状況、Mobile Endpoint Security 製品の本プライバシー ポリシー、 ライセンス契約、またはエンドユーザー契約に対する違反を調査する、防止する、または対策を講じるために、および/または Lookout、Lookout の従業員、ユーザー、ならびに一般市民の権利や財産を保護するために、そうすることが適切であると誠意をもって判断した場合は、お客様に関するデータを開示する場合があります。この場合の開示には、法執行機関、政府機関、裁判所、および／またはその他の組織との情報の共有が含まれる場合があります。

Lookout は、統合、再編、Lookout の一部資産または全資産の売却、あるいは Lookout の一部または全事業に対する他社からの融資または買収に関連して、お客様のデータを共有する場合があります。

8. 雇用主が見ることができない情報はどれですか?

Lookout は、雇用主がお客様の個人メール、閲覧履歴、連絡先、カレンダー、または個人的なテキスト メッセージの内容を閲覧することを許可しません。雇用主は、この情報が雇用主の提供する端末やネットワークを利用して送信される場合、この情報にアクセスする一定の権利を独自に保有している場合があります。しかしながら、お客様が端末で訪問するアプリケーションやサイトは、脅威を含んでいる場合や会社の方針に違反する場合を除いて、雇用主が確認することはできません。

9. データをマーケティング目的で使用することがありますか?

Lookout は、モバイル端末から自動的に収集したデータを、製品を販売したり、マーケティング目的で第三者と共有したりするために使用することはありません。ただし、端末から収集した情報を集計して調査を実施したり、モバイル端末のセキュリティや脅威にインサイトを提供したりすることがあります。このような場合、調査に含まれる集計された情報は、匿名化されます。

Lookout は、適用法に基づいて要求され、それに同意する場合に限り、お客様が Lookout に直接提供した情報や、パートナーまたはマーケティング会社等の第三者に提供した情報を使用して、Lookout が参加または主催する会議その他のイベントなど、Lookout およびその製品やサービスに関する情報を提供する場合があります。

10. Lookout はデータをどのように保護し、どれくらいの期間保存しますか?

Lookout は、管理上や技術的に有効な、物理的かつ合理的なセキュリティ対策を講じ、情報を不正アクセス、破損、または改ざんから保護しています。こうした安全対策は、Lookout が収集、処理、お

よび保存する情報の機密性を守り、かつ、テクノロジーの現状に見合うように調整されています。

Lookout では、不正な情報の開示に対する適切な安全対策を講じていますが、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、収集する情報が本プライバシーに関する方針に反する方法で開示されることが絶対にないとは保証できません。

Lookout のポリシーでは、Lookout の製品やサービスをお客様ならびに他の人々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、個人データを保持するものとしています。お客様のアカウントが使用されていない場合、および Lookout のサービス利用規約で別途定められている場合は、90 日経過後にデータを削除することがあります。情報は、バックアップまた事業継続の目的で作成されたコピーに残される場合があります。この場合、すべてのデータは業界標準の暗号化で保護されて保管されます。

11. Lookout はデータをどこに保存しますか?

Lookout は、サンフランシスコに拠点を置く企業であり、米国内にサーバーを設置しています。米国外のユーザーから収集される個人データは、米国に転送されます。米国外で Lookout の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、そこで保存ならびに処理されることがあります。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 Privacy Shield Framework の認証を受けています。Privacy Shield Principles は、EU、英国、およびスイスから受信した個人データの参加機関による使用と取り扱いについて規定する一連の要件です。Privacy Shield に加盟することで、参加者は米国法で執行可能な Principles の遵守に取り組みます。Lookout は、そのような個人データの通知、選択、外部への転送、セキュリティ、データの整合性、アクセス、執行に関して、Privacy Shield Principles に従うことを保証します。Privacy Shield に関する詳細情報、現在 Privacy Shield の下で認証を受けている企業の一覧、または Lookout の認証については、http://www.privacyshield.gov をご覧ください。

Lookout が Principles に基づく要求に従い、Privacy Shield に準じて情報を受信し、Lookout の代理機関としての役割を果たす第三者のサービス 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、および (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 に準じて一定の責任を負います。

Privacy Shield に関する質問を含め、Lookout のプライバシーに関して質問または苦情をお持ちの場合、「質問や懸念がある場合の連絡先」に示されるメールアドレスまたは住所までお問い合わせください。Lookout は、お客様と協力して問題の解決に努めます。

お客様が EU 諸国に在住で、お客様のプライバシーに関する懸念に対する Lookout の対処方法にご不満をお持ちの場合、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 へのご連絡を推奨します。Lookout はお客様の懸念を解決するため、最善を尽くします。

EU 諸国の居住者は、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、問題を解決する機会を与える、(2) 上記の Lookout が指定する独立償還請求機構の支援を求める、(3) 米国商務省に (直接または欧州データ保護機関を通して) 連絡し、商務省が問題解決を試みる時間を与える。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 の侵害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。

「お客様は自身のプライバシー設定にアクセスおよび更新することができます」と題された上記のセクションに基づいて付与される権限に加えて、一部の海外ユーザー (Privacy Shield に基づいて Lookout が情報を収集するユーザーを含む) は、Lookout が当該ユーザーに関して保有する特定の情報にアクセスしたり、当該情報を削除したりする、一定の法的権限を保持します。ユーザーは、こうした権利を行使するため、privacy@lookout.com 宛に申請を送信できます。

EU は、2018 年 5 月 25 日に発効した一般データ保護規則 (GDPR) に従って、EU 在住者のプライバシーに関する基本的な権利を保護する措置を取っています。 EU 居住者の個人データをいずれかの方法で取り扱うあらゆる機関は、データを保護する義務を負います。Lookout は、GDPR を遵守するための推奨される技術的および組織的対策を含め、商業的に合理的なあらゆる努力を払っています。

12. データの権利と選択肢にはどのようなものがありますか?

EU 諸国およびその他の特定の管轄地域の在住者は、(1) Lookout が収集する情報に対するアクセス、修正、または削除を要請する、(2) 自身の情報の処理に対する制限を要請する、(3) 自身の情報の処理に反対する、および (4) 極めて限定された状況下で特定の情報の可搬性を要請する、特定の権限を有する場合があります。これらの権限または他の権限を行使するには、雇用主 (または該当する場合は MDM プロバイダー) にお問い合わせください。下記の連絡先情報を利用して、Lookout にお問い合わせいただくことも可能です。状況に応じて、Lookout は要請を雇用主に転送し、雇用主の指示に従って対処する場合があります。フランスおよびその他の特定の管轄地域の在住者は、自分の死後その個人情報がどのような方法で保存、消去、および共有されていくかに関する指示と、該当する場合には、死後そのような権限を行使することを指定した人物に関する指示を与えることもできます。

13. Lookout のその他の質問の問い合わせ先はどこですか?

さらにご質問がある場合は、雇用主 (または該当する場合は MDM プロバイダー) に問い合わせることを推奨しています。質問を privacy@lookout.com で Lookout のプライバシー責任者に送ることも、

Lookout, Inc. の次の宛先に郵送で送ることもできます。Michael Musi, Data Privacy Officer, One Front Street, Suite 3100, San Francisco, CA 94111.EU 諸国の在住者である場合は、次の宛先にメールすることで、Lookout, Inc. までご連絡ください。G.J.Schenk、SVP International Sales、Florapark 3, 2012 HK Haarlem、Netherlands.

発効日:2019 年 4 月 15 日