



Appleと教育

プライバシーに関する保護者向けガイド

このガイドは、Appleがどのように生徒の情報を守っているのか、保護者のみなさんの理解を深めるために作成されています。Appleは、最適な学習用ツールを提供するとともに、生徒のプライバシーを保護し、そのデータの安全性を維持しつつ、Appleのテクノロジーが動作する状態を確保することを目標としています。プライバシーとセキュリティは、Appleのハードウェア、ソフトウェア、サービスの設計に欠かせない要素です。生徒の情報に関するAppleのポリシーは以下の通りです。

- 生徒の情報を販売することはありません。また、マーケティング目的や広告目的で他社と共有することはありません。
- Eメールの内容やウェブのブラウズ履歴を基に生徒のプロファイルを構築することはありません。
- 関連する教育向けサービスを提供する目的以外に、生徒の個人情報を、収集、使用、開示することはありません。

このガイドでは、生徒の体験に関連する以下のカテゴリについてプライバシーの詳細を説明しています。学校が所有するiPadまたはMacを生徒に提供している場合にも、生徒が個人のデバイスを学校に持ち込んでいる場合にも対応します。

- **生徒のアカウント** — 生徒がサービスやその他の学習教材にアクセスする際に使用するAppleのID。
- **生徒のデータ** — 保存されている生徒の情報、生徒がデジタルで作業をすることにより生成される情報。
- **デバイス管理** — 生産性の高い学習環境を実現するために、学校がiPadやMacを設定し管理する方法。
- **デジタル市民権** — 学校や自宅でのテクノロジー利用のベストプラクティス。

生徒のアカウント

iPadやMacは、生徒のロッカーや机、実験室の作業台のように、あらゆる教材や学校の課題に簡単にアクセスできる場所です。例えば、iPadやMacで教材を読み、ノートを取ることや、マルチメディアプロジェクトを作成して科学実験を記録することもできます。作業を保存したり、ほかのAppleリソースにアクセスするには、Appleアカウントが必要です。アカウントには2種類あります。1つは、単にApple IDと呼ばれる一般消費者向けアカウント、もう1つは、管理対象Apple IDという学校用に設計されたアカウントです。このガイドでは、管理対象Apple IDに焦点を当てます。

管理対象Apple ID

管理対象Apple IDは、一般消費者向けApple IDと異なり、学校や自治体に所有、管理され、購入や通信の制限などの学校特有のニーズに応じています。管理対象Apple IDは、iPadやMac、iCloud、Appleのクラウドサービス、iTunes UといったAppleサービスへのサインインに使用します。Apple Pay、HomeKit、iPhoneを探すなどのAppleサービスについては、管理対象Apple IDでは利用できません。また、App Store、iTunes Store、Apple Musicでの生徒による購入にも対応していません。

学校は、プライバシーとセキュリティを保ちつつ、生徒用の管理対象Apple IDを作成することができます。このIDは、幅広く採用されているセキュリティ手法である2ファクタ認証を使用して構築されています。生徒のプライバシーを維持するため、管理対象Apple IDが使用する生徒の情報の量は限られています。例えば、アカウント作成時に管理対象Apple IDに関連づけられるデータは、生徒の名前、学年、クラス、生徒IDに限られます（学校は任意で生徒のEメールアドレスや写真を設定することができます）。学校が保持する生徒に関するその他のデータは、学校のStudent Information System (SIS) に別途保存されます。

管理対象Apple IDは、個人所有のiPadやMacで学校の課題を行うために使用することもできます。自宅で宿題をする場合、生徒は自分の管理対象Apple IDと、学校が発行した2ファクタ認証対応の自宅用パスワードを使ってiCloudにサインインすることができます。自宅であっても、生徒が個人所有のデバイスで管理対象Apple IDを使った場合には、学校はFaceTimeやiMessageといった機能の利用を制限することができます。注意：生徒が管理対象Apple IDでサインインしている時に作成するiCloud書類は、下記で説明する通り、監査・監視の対象にもなります。

管理対象Apple IDは、学校の環境で使用するためのIDです。学校外では、13歳以上の生徒(管轄区域により異なります)は、個人のApple IDを作成すれば、Appleが販売する製品やサービスを利用することができます。13歳以下の生徒はファミリー共有で家族に付帯してApple IDを持つことができます。

生徒が個人のApple IDを使って学校管理のデバイスにログインすることが適切であると学校が判断する場合、ログインに使用する個人のApple IDは、Appleのプライバシーポリシーとサービスの追加条項の対象になります。従って学校は、個人のApple IDの使用が、適用される国内法と学校のポリシーに適合するようにならなければなりません。

管理対象Apple IDを監査・監視する

管理対象Apple IDは、学校の裁量で生徒のアカウントの監査・監視を実施する機能に対応しています。この機能は、すべての監査を記録する厳密なプロトコルを備えています。これは、Appleが提供するITポータルであるApple School Managerで管理者、マネージャー、教師に監査権限を与えることで機能します。学校がアカウントを調査すると、監査担当者の認証情報、日付とともに記録されます。監査期間中、監査担当者は、iCloudに保存されたコンテンツやiCloudにデータを保存するアプリケーションを閲覧したり、修正することができます。監査許可は7日を経過すると期限が切れます。必要な場合には、保護者は学校管理者と連携して生徒のアカウントを監査することができます。

コミュニケーション：テキストメッセージ、Eメール、ボイスチャット、ビデオチャット

管理対象Apple IDはEメールに使用できません。Appleのメッセージングサービス、ビデオチャットサービスであるiMessageとFaceTimeは、デフォルトで無効になっています。この2つの機能は学校側で有効に設定できますが、その場合、関連づけられている条件に従って利用する必要があります。学校のEメールおよび電子通信ポリシーを確認するには、学校管理者に問い合わせてください。

生徒のデータ

今日では生徒は、iPadやMacを使って授業のノートをとったり、スケッチ、デザイン、コードを書いたり、アニメーションを作ったり、記録したり、課題を仕上げる事が出来ます。生徒の個人情報を守り、安全な状態に保つため、Appleでは「必要最低限のデータ」というアプローチでデータを取り扱っています。以下では、位置情報、セキュリティ、所有権、コマーシャルアクティビティ、コンプライアンスに関する生徒のデータの取り扱い方の例を紹介します。

位置情報

位置情報サービスを利用すると、位置情報アプリケーションとウェブサイトで位置データを使用できます。例えば、生徒が理科の授業や校外学習で、世界中の鳥の種類をマッピングする必要があるとします。デバイスの初期設定の際に、生徒は設定アシスタントで位置情報サービスを有効に設定することができます。学校支給のデバイスについては、学校のMobile Device Management (MDM) ソリューションでこの設定を非表示にすることができ、位置情報サービスはデフォルトで無効に設定されます。Appleでは、位置データをどのように使用するかをアプリケーションごとに細かく制御できる機能を提供しています。生徒は、これらの設定を一切許可しない、使用時に許可する、常に許可するのいずれかに設定できます。

生徒がデバイスを使用する中で、様々なアプリケーションが位置情報サービスを有効にするよう促すことがあるでしょう。常にアプリケーションが位置情報サービスにアクセスできるように設定している場合には、時々リマインダーが表示されます。設定はいつでも変更することができます。

デバイスでのセキュリティとクラウドでのセキュリティ

生徒が文書を作成したり、コンテンツを使って学んだり、授業のアクティビティに取り組む際に、生徒のプライバシーが確実に守られ、自分の学習内容を安全に保存できることが非常に重要です。Appleのサービスは、セキュリティとプライバシーを念頭に置いて構築されているため、生徒がデバイスを使用する前、使用している最中、使用した後のどのタイミングでも、生徒と学校のデータは確実に保護されます。

データについて考える際には、デバイス上のデータとクラウドに保存されているデータの2つの領域に分けて考えることをおすすめします。複数の生徒が1台のiPadを交代で使いながらパーソナルな学習体験を可能にするiOSの機能である「共有 iPad」を利用している学校の場合、それぞれの生徒は、授業を終える前に、管理対象Apple IDを経由して自分の学習内容と設定をiCloudに保存することになります。学習内容は自動的にiCloudに保存され、同じiPadを共有するほかの生徒はアクセスできません。

生徒の学習内容のデータはデバイス上で暗号化され、iPadやMacで安全に保存されます。iPadでは、自動的に暗号化が有効になります。MacではFileVaultで有効にすることができます。そのため、デバイス上のデータにアクセスするには生徒のパスワードが必要です。

AppleのクラウドサービスであるiCloudでは、データの場所を移動する際には必ずHTTPSという安全なネットワークプロトコルが必要となります。iCloudは業界標準のセキュリティ手段に従って構築されており、データ保護のための厳格なポリシーを採用しています。iPadやMacでは、サービスやインターネットに接続する際、暗号化接続も必要です。

iCloudではユーザーのデータを保護するために、データをインターネット経由で送信する際にはデータの暗号化、サーバに保管しておく間は暗号化形式での保存、認証にはセキュアトークンを使用します。このように、生徒のデータはデバイスに送信されている時もiCloudに保存されている時も不正アクセスから保護されます。iCloudでは、大手金融機関と同じレベルの暗号化セキュリティを採用しており、暗号化キーはいかなる第三者にも提供されることはありません。Appleは、自社のデータセンターにおいて暗号鍵を保持しています。また、生徒のパスワードと資格情報は、Appleが読んだりアクセスしたりできない方法でiCloudに保存されています。

iCloudのセキュリティとプライバシーの詳細については、<https://support.apple.com/ja-jp/HT202303>を参照してください。

データの所有権

Appleは、デバイスやクラウド上で生徒のデータを所有していません。学校や自治体は、生徒がデバイスからいつどのようにサービスやコンテンツにアクセスするかを制御することができますが、生徒の学習内容はそのまま生徒自身が所有します。詳細については、学校のデータプラクティスポリシーの詳細を参照してください。

Student Privacy Pledge

Student Privacy Pledgeは、Future of Privacy Forum (FPF) およびSoftware & Information Industry Association (SIIA) が生徒のプライバシーを保護する目的で導入した誓約です。AppleはStudent Privacy Pledgeに署名しています。詳細については、[Student Privacy Pledge](#)を参照してください。

グローバルコンプライアンス

Appleは、世界中の学校と協力して、学習向けの最適なテクノロジーを提供しており、[ISO 27001認証 \(情報セキュリティ\)](#)を取得しました。Apple School Managerや管理対象Apple ID、iTunes U、iCloudを使用する場合、個人データが国外に保管されることがあります。どこに保管した場合でも、データには共通の厳格なデータ保管の標準と要件が適用されます。

デバイスの管理

学習環境をサポートするために学校が生徒のiPadやMac、そこにインストールされているアプリケーションやブックを設定し、管理する可能性は多いにあることでしょう。デバイス管理ソリューションを利用すれば、学校所有のデバイスに加え、生徒が学校に持ち込む個人のデバイスでも確実にポリシーと設定を確立することができます。このセクションでは、生徒の情報を安全に守る一般的なデバイス管理用ツールに触れます。生徒が使用するiPadやMacの所有者が誰であるかによって学校が管理する機能が変換することがあるため、それを把握しておくことも重要です。

学校においては、基本的に3つの所有権のシナリオがあります。

- **1人1台の導入**：学校がiPadやMacを購入して、各生徒に提供。このタイプの導入は、特定の学年や学部、または自治体や大学全体に対して行うことができます。
- **共有使用の導入**：生徒が交代で使用するiPadやMacデバイスのセットを学校が購入して提供。
- **個人デバイスの持ち込みによる導入 (BYOD)**：保護者がiPadやMacを生徒個人のデバイスとして購入し、学校や大学で使用。

デバイスを管理する

生徒のデバイスはMobile Device Management (MDM) ソリューションで管理することができます。MDMは第三者企業が提供するサービスで、デバイスの設定とリソースを管理するためのソフトウェアを提供しています。MDMを使用すると、アプリケーション、ブック、その他学校が提供する教育コンテンツをインストールし、デバイスを生徒用に設定することができます。学校のIT管理者は、iPadやMac、アプリケーション、学校のネットワークで有効または無効にできる機能についてポリシーを設定することができます。MDMソフトウェアは、通常は学校所有のデバイスの管理に使用されますが、必要に応じてBYODのシナリオにも使用します。

生徒が学校所有のデバイスを使用している場合、iPad やMacのMDM設定で、設定を削除できないようにすることができます。これは、多くの1人1台の導入および共有使用導入のシナリオにおいて標準的になっています。また、共有 iPad機能を使用する場合MDMは必須です。

生徒が個人デバイスを学校に持ち込む場合は、学校の管理ソフトウェアに登録する必要があります。この場合には、デバイスが学校の所有でないため、生徒や保護者側でMDMデバイスの設定を削除することができます。

IT管理者は、管理下にあるAppleデバイスに保存されている生徒のデータと位置情報に限定的アクセスすることができます。MDMソフトウェアでは生徒のデバイス上のすべてを見ることはできません。設定を行ったり、アプリケーションをインストールするのに使用される通知を通じてのみ、デバイスとやり取りできます。これによって、生徒のデバイスの監視や追跡を防止することができます。デバイスがなくなったり盗まれたりした場合、IT管理者は、Managed Lost Modeという機能を使って、リモートでデバイスを探すことができます。これはデバイスが紛失し、その位置にアクセス中であることをユーザーに通知するメッセージがデバイスに送信された後に限られます。管理者がManaged Lost Modeをオフにすると、ロック画面のメッセージとホーム画面の警告の両方でユーザーに通知されます。

Apple School Managerと生徒の情報

AppleのIT向け管理ポータル、Apple School Managerは、生徒のプライバシーを念頭に置いて構築されています。例えば、Apple School Managerは基本アカウントとクラス名簿の設定に必要なデータのみをインポートし、学校が持つその他の生徒の情報はインポートしません。学校は、Apple School Managerを使って生徒、教師、その他のスタッフが使用する管理対象Apple IDを作成できます。

デバイスを構成する

学校は、特定の学年やカリキュラム計画の要件を満たすためにどのようにiPadやMacを構成するかを決定します。アプリケーションやコンテンツの設定を実行するためには、どの設定、機能、アプリケーションを使用するかを指示するファイルをデバイスに送ります。このファイルは構成プロファイルと呼ばれており、学校が管理します。学校がMDMを利用していない場合は、学校管理者から構成プロファイルをダウンロードできるリンクをEメールで送信するか、または、Macで利用できるApple Configuratorというツールを使って、各デバイスに手動でプロファイルをインストールします。

1人1台の導入では、MDMを利用してデバイスの設定や管理を行うのが最も一般的です。生徒は始業日に、管理対象Apple IDとともにデバイスを受け取ることになります(管理対象Apple IDとMDMの詳細については、1ページの「生徒のアカウント」セクションを参照してください)。

共有使用の導入については、標準的なアプリケーションや学習教材のセットをインストールして、一般的な方法でデバイスを設定することになるでしょう。生徒がApple IDでログインする必要がない共有使用の導入もありますが、iOS 9以降では、共有 iPad機能によりiPadを各生徒向けにパーソナライズすることができます。学校が作成した管理対象Apple IDを使ってこのマルチユーザーモードにアクセスすることで、毎回授業でiPadを使用するたびに、生徒は自分の学習内容や設定を保存することができます。共有 iPadにより各生徒のデータはデバイスやiCloudに安全に保存され、保護されます。

管理対象でないデバイス

生徒が個人のiPadやMacを学校で使用している場合 (BYOD)、学校がデバイスを管理する必要はありませんが、学校によっては個人所有のデバイスを使用している生徒にも学校が提供する管理ソフトウェアに登録させる場合もあります。学校によってポリシーが異なりますので、BYODプログラムでどのようにデバイスが管理されているかについて、それぞれの学校の管理者に確認してください。

クラスルームアプリケーション

クラスルームは、iPadを使った授業での指導に役立つAppleのiPadアプリケーションです。教師は、このアプリケーションを使ってクラスの各生徒のiPadにインストールされている特定のアプリケーションを起動したり、ウェブサイトと共有したりできます。また、アクティビティグループを作ったり、Screen Viewを使って生徒の画面を見ることがもできます。さらに、AirPlayとApple TVを使うと、1人の生徒の画面をクラス全体で共有することもできます。生徒が学習に集中できるようにするため、教師は使用できるアプリケーションを1つにするようデバイスをロックしたり、一時的に教室内のすべてのデバイスの画面をロックしたりすることができます。

クラスルームアプリケーションは、教師向けの優れたツールとして設計されていますが、同時に透明性と生徒のプライバシーのベストプラクティスを実現する設計にもなっています。つまり、生徒のiPadデバイスはクラスの中でのみ管理が可能です。教室外で教師が生徒のデバイスを管理したり、閲覧したりすることはできません。透明性を確保するため、クラスの生徒の画面でScreen Viewがアクティブになっている時は、生徒の画面の上部に画面が見られていることを示す通知が表示されます。学校は、Screen Viewを無効にして、教師が生徒の画面を見ることができないように設定することもできます。

デジタル市民としてのあり方

安全かつ責任ある方法でテクノロジーを利用できる能力のことをDigital Citizenship (デジタル・シティズンシップ)と呼びます。インターネットの安全、通信、ネットいじめ、情報リテラシー、原作者のクレジット表記、著作権などについてのガイダンスなどが含まれます。現在の学びのあり方は、たった数年前と比べても大きく変わりつつあるため、学校がこれらに関するベストプラクティスを導入することが重要です。生徒、教師、スタッフ、その他学校に関わるコミュニティの全員がデジタル市民としてのあり方についてのトレーニングを受けるべきでしょう。

生徒が良きデジタル市民となる助けとなり、学校や保護者の知識向上に役立つ資料が公開されています。Common Sense Mediaでは、学校やコミュニティ向けの教材を提供しています。保護者と生徒のみならず、許容される使用、Eメール、デバイスの保管と充電、コンテンツやアプリケーションへのアクセスなどに関する学校のテクノロジーポリシーを再確認することをおすすめします。

デジタルシティズンシップに関連するリソース

一般社団法人モバイルコンテンツ審査・運用監視機構(EMA) : <http://ema-edu.jp/index.html>

Future Privacy Forumの生徒のデータプライバシーに関する保護者向けガイド (英語) : <https://ferpasherpa.org/parents/a-parents-guide-to-student-data-privacy/>

Common Sense Media (英語)

- デジタルシティズンシップ : <https://www.commonsensemedia.org/educators/digital-citizenship>
- 家族向けガイド : <https://www.commonsensemedia.org/guide/essentialbooks>
- アプリケーションガイド : <https://www.commonsensemedia.org/guide/best-first-kids-apps>

関連情報

生徒のセキュリティとプライバシーを保護するApple製品の詳細については、以下のリソースを参照してください。
プライバシーに関するご質問がある場合は、www.apple.com/jp/privacy/contactからAppleに直接お問い合わせください。

- あなたのプライバシーに関するAppleの取り組み : www.apple.com/jp/privacy
- 教育機関向けデータとプライバシーに関する概要 : http://images.apple.com/jp/education/docs/Education_Privacy_Schools_May16.pdf
- Apple School Managerヘルプ : <https://help.apple.com/schoolmanager>
- iCloud のセキュリティおよびプライバシー : <https://support.apple.com/ja-jp/HT202303>
- Appleでのペアレンタルコントロール : <https://support.apple.com/ja-jp/HT201304>
- iTunes Uのセキュリティとプライバシー : <https://support.apple.com/ja-jp/HT204918>

