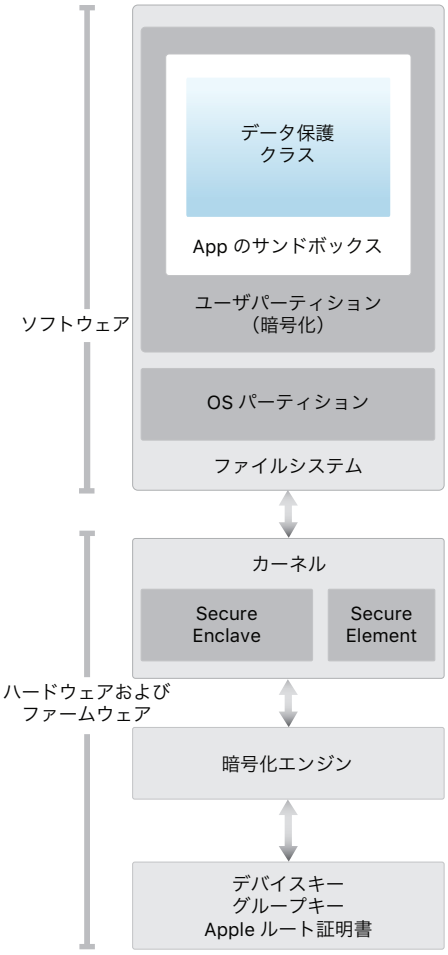
iOS のセキュリティ

iOS 12.1

2018 年 11 月

目次

概要



iOS のセキュリティアーキテクチャの図。この文書で説明するテクノロジーの概要を視覚的に表したものです。

Apple の iOS プラットフォームは、セキュリティを核に据えて設計されています。数十年に及ぶ経験を出発点に最高のモバイルプラットフォームの開発に取り掛かり、まったく新しいアーキテクチャを構築しました。デスクトップ環境のセキュリティハザードを念頭に置き、iOS の設計では、セキュリティに対する新たなアプローチを確立しました。モバイルセキュリティを強化し、デフォルトでシステム全体を保護する革新的な機能を開発し、統合しました。その結果、iOS ではモバイルデバイスのセキュリティが大きく進歩しています。

すべての iOS デバイスでは、ソフトウェア、ハードウェア、およびサービスを連携して機能するように統合することで、最高のセキュリティと透過的なユーザ体験を実現しています。iOS はデバイスやデータのみを保護するのではなく、エコシステム全体を保護します。これにより、ローカル上、ネットワーク上および主なインターネットサービス上でのすべてのユーザ操作が保護されます。

iOS および iOS デバイスには、高度でありながら使いやすいセキュリティ機能が搭載されています。これらのほとんどの機能はデフォルトで有効になっており、IT 部門で何から何まで構成する必要はありません。また、デバイスの暗号化などの重要なセキュリティ機能をユーザが誤って無効にしないように、そのような機能の設定は変更できないようになっています。Face ID などの機能も搭載することで、デバイスの保護がさらに簡単で直観的になり、ユーザ体験も向上します。

この文書では、iOS プラットフォームにおけるセキュリティ技術とセキュリティ機能の実装方法について詳しく説明します。また、組織特有のセキュリティのニーズを満たすために、iOS プラットフォームのセキュリティ技術とセキュリティ機能を組織独自のポリシーや手順と統合する場合に役立てることもできます。

この文書は、以下のトピックに分かれています。

- **システムのセキュリティ：**iPhone、iPad、および iPod touch のプラットフォームとして統合された安全なソフトウェアおよびハードウェア。
- **暗号化とデータ保護：**デバイスを紛失したり盗まれたりした場合や、不正なユーザが使用したり変更したりしようとした場合でもユーザデータを保護するアーキテクチャと設計。
- **App のセキュリティ：**プラットフォームの完全性を損ねることなく安全に App を実行するシステム。
- **ネットワークのセキュリティ：**安全な認証と転送データの暗号化を可能にする業界標準のネットワークプロトコル。
- **Apple Pay：**Apple が導入した安全な支払いのための機能。
- **インターネットサービス：**メッセージ、同期、およびバックアップを支える Apple のネットワークベースのインフラストラクチャ。
- **ユーザパスワード管理：**パスワード制限、および許可したソースによるパスワードアクセス。
- **デバイスの管理：**iOS デバイスを管理し、不正使用を防ぎ、紛失または盗難時にリモートワイプを可能にする方法。
- **プライバシーコントロール：**位置情報サービスおよびユーザデータへのアクセスを制御するために使用される iOS の機能。
- **セキュリティに関する認証とプログラム：**ISO 認証、暗号認定、コモンクライテリア認証、および Commercial Solutions for Classified（CSfC）に関する情報。

システムのセキュリティ

DFU（デバイス・ファームウェア・アップグレード）モードにする

デバイスを DFU モード（リカバリモード）にした後にデバイスを復元すると、Apple が署名した未変更のコードしか存在しない、既知の正常な状態に戻ります。手動で DFU モードにできます。

まず、USB ケーブルを使ってデバイスをコンピュータに接続します。

次に、デバイスに応じて以下の操作を行います。

iPhone X 以降、iPhone 8、iPhone 8 Plus：音量を上げるボタンを押してすぐに離してから、音量を下げるボタンを押してすぐに離します。次に、サイドボタンを押したままにして、音量を下げるボタンを押します。5 秒後にサイドボタンを離し、音量を下げるボタンはリカバリモード画面が表示されたら離します。

iPhone 7、iPhone 7 Plus：サイドボタンと音量を下げるボタンを同時に押したままにして、サイドボタンを離し、音量を下げるボタンはリカバリモード画面が表示されたら離します。

iPhone 6s 以前、iPad、iPod touch：ホームボタンとトップ（またはサイド）ボタンを同時に押したままにして、トップ（またはサイド）ボタンを離し、ホームボタンはリカバリモード画面が表示されたら離します。

注意：デバイスが DFU モードのときは、画面に何も表示されません。Apple ロゴが表示された場合は、サイドボタンまたはスリープ／スリープ解除ボタンを長く押しすぎです。

システムのセキュリティは、すべての iOS デバイスのあらゆるコアコンポーネントでソフトウェアとハードウェアの両方のセキュリティが保たれるように設計されています。システムのセキュリティには、起動プロセス、ソフトウェア・アップデート、Secure Enclave などがあります。このアーキテクチャは iOS のセキュリティの中核であり、デバイスの使いやすさが損なわれることはありません。

iOS デバイスではハードウェア、ソフトウェア、サービスが密接に統合されているため、各システムコンポーネントの信頼性の確保や、システム全体の検証が可能になっています。iOS の初回起動からソフトウェア・アップデート、さらに他社製 App の使用に至るまで、ハードウェアとソフトウェアが最適な形で連動し、リソースが適切に使用されるように、各ステップが解析および検証されます。

セキュアブートチェーン

起動プロセスの各ステップに含まれるコンポーネントには、完全性を保証するために Apple によって暗号化された署名が付いており、信頼チェーンの検証後にのみ実行されます。これらのコンポーネントには、ブートローダー、カーネル、カーネル機能拡張、ベースバンドファームウェアなどがあります。このセキュアブートチェーンにより、最下位レベルのソフトウェアが改ざんされていないことが保証されます。

iOS デバイスの電源を入れると、デバイスのアプリケーションプロセッサによって、**Boot ROM** という読み出し専用メモリから即座にコードが実行されます。ハードウェアの信頼の起点となるこの変更不可のコードは、チップ製造時に書き込まれたものであり、無条件に信頼されます。Boot ROM コードには Apple ルート CA の公開鍵が含まれており、この公開鍵は、iBoot ブートローダーの読み込みを許可する前に iBoot ブートローダーが Apple によって署名されていることを確認するために使用されます。これが信頼チェーンの最初のステップです。信頼チェーンの各ステップでは、その次のステップが Apple によって署名されていることを確認します。iBoot のタスクが終了すると、iOS カーネルが検証および実行されます。A9 以前の A シリーズプロセッサを搭載したデバイスではもう 1 つ段階が加わり、Boot ROM によって **Low-Level Bootloader（LLB）**が読み込まれて検証された後に、iBoot が読み込まれて検証されます。

Boot ROM で LLB（古いデバイスの場合）または iBoot（新しいデバイスの場合）の読み込みができない場合は、デバイスが DFU モードになります。LLB または iBoot で次のステップの読み込みまたは検証ができない場合は、起動が停止され、デバイスに「iTunes に接続」という画面が表示されます。これはリカバリモードと呼ばれます。いずれの場合も、USB 経由でデバイスを「iTunes」に接続し、工場出荷時の設定に復元する必要があります。

モードに応じてユーザデータへのアクセスを制限するために、Secure Enclave によって**ブート・プログレス・レジスタ（BPR）**が使用されます。このレジスタが更新された後に、以下のモードに入ります。

- **リカバリモード：**Apple A10、S2、およびそれ以降の **System on Chip（SoC）**を搭載したデバイスで iBoot により設定されます
- **DFU モード：**A12 SoC を搭載したデバイスで Boot ROM により設定されます

詳しくは、この文書の「暗号化とデータ保護」セクションを参照してください。

モバイルデータ通信ネットワークにアクセスできるデバイスでは、ベースバンドサブシステムでも、署名されたソフトウェアおよびベースバンドプロセッサによって検証された鍵を使って、これと似た固有のセキュアブートプロセスが実行されます。

さらに Secure Enclave コプロセッサでも、Secure Enclave の独立したソフトウェアが Apple によって検証および署名されていることを確認するために、セキュアブートプロセスが実行されます。詳しくは、この文書の「Secure Enclave」セクションを参照してください。

手動でリカバリモードにする方法について詳しくは、次の Web サイトを参照してください。
support.apple.com/kb/HT1808

システムソフトウェア認証

Apple は、新たなセキュリティ上の懸念に対処したり、新しい機能を提供したりするために、定期的にソフトウェア・アップデートをリリースしています。これらのアップデートは、サポートされているすべてのデバイスに同時に提供されます。ユーザは、iOS アップデートの通知をデバイスまたは「iTunes」で受け取ります。アップデートはワイヤレスで配信されるので、最新のセキュリティ修正の迅速な導入を促すことができます。

前述の起動プロセスにより、Apple が署名したコードのみデバイスにインストールされることが保証されます。最新のセキュリティアップデートを含まない古いバージョンにデバイスがダウングレードされるのを防ぐため、iOS はシステムソフトウェア認証というプロセスを使用します。ダウングレードが可能になってしまうと、デバイスを乗っ取った攻撃者に古いバージョンの iOS をインストールされ、新しいバージョンで修正された脆弱性を悪用されてしまいます。

Secure Enclave を搭載したデバイスでは、ソフトウェアの完全性を保証し、ダウングレード目的のインストールを防止するために、Secure Enclave コプロセッサでもシステムソフトウェア認証が利用されます。詳しくは、この文書の「Secure Enclave」セクションを参照してください。

iOS ソフトウェア・アップデートは、「iTunes」から、またはワイヤレス（OTA）でデバイスにインストールできます。「iTunes」を使用する場合は、iOS の完全なコピーがダウンロードされインストールされます。ワイヤレスでソフトウェア・アップデートする場合は、アップデートの完了に必要なコンポーネントのみがダウンロードされるため、iOS 全体をダウンロードする場合よりもネットワーク効率が向上します。さらに、macOS High Sierra 以降を搭載しコンテンツキャッシュを有効にしている Mac にソフトウェア・アップデートをキャッシュすれば、iOS デバイスで必要なアップデートをインターネット経由で再ダウンロードする必要がなくなります。その場合でも、アップデートプロセスを完了するために、デバイスから Apple のサーバに接続する必要はあります。

iOS のアップグレード中は、「iTunes」（OTA でのソフトウェア・アップデートの場合はデバイス自体）が Apple のインストール認証サーバに接続して、インストールされるバンドルの各コンポーネント（iBoot、カーネル、および OS イメージなど）の暗号処理による計算値のリスト、アンチリプレイの乱数（ノンス）、およびデバイス固有の **ECID（Exclusive Chip Identification）**を送信します。

認証サーバは、提示された暗号計算値リストとインストールが許可されているバージョンを照合し、一致が見つかった場合は、ECID を計算値に追加して結果に署名します。署名されたデーター式は、アップグレードプロセスの一部としてサーバからデバイスに送信されます。ECID を追加することで、リクエストしたデバイスの認証を「パーソナライズ」することができます。既知の計算値に対してのみ認証および署名することで、サーバは Apple からの指示通りの正確なアップデートの実行を保証します。

起動時に信頼チェーンで評価することで、署名が Apple のものであるかどうか、さらに、ディスクから読み込んだ項目の計算値とデバイスの ECID の組み合わせが署名されたものと一致するか、検証されます。これらのステップにより、認証がそのデバイス固有のものであることが保証されるので、あるデバイスの旧バージョンの iOS を別のデバイスにコピーできなくなります。また、ノンスが使用されるため、攻撃者がサーバの応答を保存し、それを使ってデバイスを不正に解析したり、システムソフトウェアを改ざんしたりすることもできません。

Secure Enclave

Secure Enclave は、System on Chip（SoC）に組み込まれたコプロセッサです。暗号化されたメモリを使用するほか、ハードウェア乱数ジェネレータを備えています。Secure Enclave は、**データ保護**のための鍵管理のすべての暗号演算を担い、カーネルが危殆化した場合でもデータ保護の完全性が維持されます。Secure Enclave とアプリケーションプロセッサ間の通信は、割り込み方式のメールボックスと共有メモリのデータバッファによって隔離されています。

Secure Enclave は、専用の Secure Enclave Boot ROM を備えています。アプリケーションプロセッサの Boot ROM と同様に、Secure Enclave Boot ROM も、Secure Enclave にとってハードウェアの信頼の起点となる変更不可のコードです。

Secure Enclave は、Apple がカスタマイズした L4 マイクロカーネルをベースにした Secure Enclave OS を実行します。Secure Enclave OS は Apple によって署名されており、Secure Enclave Boot ROM によって検証され、パーソナライズされたソフトウェア・アップデート・プロセスを通じてアップデートされます。

デバイスが起動すると、Secure Enclave Boot ROM によって一時的なメモリ保護キーが作成されます。これは、デバイスの UID と関連付けられて、デバイスのメモリ領域の Secure Enclave 部分の暗号化に使用されます。Apple A7 以外では、メモリ保護キーで Secure Enclave のメモリの認証も行われます。A11 以降および S4 SoC では、完全性ツリーを使用することでセキュリティが不可欠な Secure Enclave のメモリのリプレイを防止しますが、これはオンチップ SRAM に保存されたメモリ保護キーおよびノンスによって認証されます。

Secure Enclave によりファイルシステムに保存されたデータは、UID と関連付けられたキーおよびアンチリプレイカウンタを使用して暗号化されます。アンチリプレイカウンタは、専用の不揮発性メモリ**集積回路（IC）**に保存されます。

A12 または S4 SoC を搭載したデバイスでは、Secure Enclave がアンチリプレイカウンタ保存用のセキュアストレージ集積回路（IC）とペアリングされます。セキュアストレージ IC は、変更不可の ROM コード、ハードウェア乱数ジェネレータ、暗号化エンジン、および物理的改ざん防止を考慮して設計されています。カウンタを読み取るときやアップデートするときは、Secure Enclave とストレージ IC で、カウンタへの排他的アクセスを確保するためのセキュアプロトコルが用いられます。

アンチリプレイの境界線を示すイベントでのデータの破棄には、Secure Enclave 上のアンチリプレイサービスが使用されます。これに該当するイベントの一部を以下に示します。

- パスコードの変更
- Touch ID または Face ID の有効化／無効化
- 指紋の追加／削除
- Face ID のリセット
- Apple Pay カードの追加／削除
- すべてのコンテンツと設定を消去する

Secure Enclave は、Touch ID センサーおよび Face ID センサーからの指紋データや顔認識データの処理にも関与します。登録データと一致するかどうかを確認し、一致する場合はユーザに代わってアクセスや購入を許可します。

OS 整合性保護

カーネル整合性保護

iOS のカーネルで初期化が完了すると、カーネルおよびドライバのコード改ざんを防ぐために、カーネル整合性保護（KIP）が有効になります。**メモリコントローラ**は保護された物理メモリ領域を割り当て、**iBoot** はこれを使用してカーネルおよびカーネル機能拡張を読み込みます。ブート完了後は、メモリコントローラによって、この保護された物理メモリ領域への書き込みが拒否されます。さらに、アプリケーションプロセッサのメモリ管理ユニット（MMU）が構成され、保護メモリ領域外の物理メモリからの特権コードのマッピング、およびカーネルメモリ領域内での物理メモリの書き込み可能なマッピングが禁止されます。

KIP の有効化に使用されるハードウェアは、構成変更を防ぐため、ブートプロセス完了後にロックされます。KIP は、Apple A10 および S4 以降の SoC でサポートされます。

システムコプロセッサ整合性保護

システムコプロセッサは、アプリケーションプロセッサと同じ SoC 上にある CPU です。特定の目的専用に設計されており、iOS のカーネルからさまざまなタスクが委譲されます。たとえば、以下のものがあります。

- Secure Enclave
- イメージ・センサー・プロセッサ
- モーションコプロセッサ

コプロセッサのファームウェアによって多数の重要なシステムタスクが処理されるため、そのセキュリティはシステム全体のセキュリティを大きく左右します。

システムコプロセッサ整合性保護（SCIP）では、カーネル整合性保護と同じようなメカニズムによってコプロセッサのファームウェア改ざんが防止されます。起動時に、iBoot によって、KIP 領域とは別の予約済み保護メモリ領域に各コプロセッサのファームウェアが読み込まれます。また、各コプロセッサのメモリ管理ユニットが構成され、以下の操作が禁止されます。

- 保護メモリ領域の該当部分外での実行可能なマッピング
- 保護メモリ領域の該当部分内での書き込み可能なマッピング

Secure Enclave の SCIP の構成は、起動時に Secure Enclave OS によって行われます。

SCIP の有効化に使用されるハードウェアは、構成変更を防ぐため、ブートプロセス完了後にロックされます。SCIP は、A12 および S4 以降の SoC でサポートされます。

ポインタ認証コード

ポインタ認証コード（PAC）は、メモリ破壊バグの悪用防止に使用されます。システムソフトウェアおよび内蔵 App は、PAC を使用して関数ポインタとリターンアドレス（コードポインタ）の改ざんを防止します。これは多くの攻撃に対する障壁となります。たとえば、スタックに格納された関数のリターンアドレスを改ざんすることによって既存のコードを不正に実行させようとする ROP（Return Oriented Programming）攻撃に対して有効です。

PAC は、A12 および S4 SoC でサポートされます。

Touch ID

Touch ID は、iPhone や iPad への安全なアクセスをより速く、より簡単にする指紋認証システムです。あらゆる角度から指紋を読み取り、継続的にユーザの指紋について学習を進めるテクノロジーです。使用するたびに新たなノードの重複をセンサーで検出することにより、指紋マップを拡張し続けます。

Face ID

Face ID 対応の Apple デバイスでは、デバイスに顔を向けるだけでロックを安全に解除できます。TrueDepth カメラシステムを使用した高度な技術によって顔の形状を正確に読み取ることで、直感的かつ安全な認証を実現します。Face ID では、ニューラルネットワークを使用してユーザが注視しているかどうかの判断、照合、およびなりすまし防止の処理が行われるため、デバイスを見つめるだけでロックを解除できます。Face ID は、外見の変化に自動的に適応し、生体データのプライバシーとセキュリティもしっかりと守られます。

Touch ID、Face ID、パスコード

Touch ID または Face ID を使用するには、パスコードでロック解除するようにデバイスを設定する必要があります。Touch ID または Face ID で認証に成功すると、デバイスのパスコードを入力しなくてもロックが解除されます。これによって、ユーザがパスコードを入力する頻度が減るため、長くて複雑なパスコードもはるかに実用的なものとなります。Touch ID や Face ID は、

パスコードに取って代わるのではなく、適度な使用範囲と時間の制約の中でデバイスへの簡単なアクセス方法を提供するものです。強力なパスコードは iOS デバイスによるデータ暗号化保護の基礎となるため、これは重要な点です。

いつでも Touch ID や Face ID の代わりにパスコードを使用できます。また、以下の操作では常に生体認証ではなくパスコードによる認証が求められます。

- ソフトウェアのアップデート。
- デバイスの消去。
- パスコード設定の表示と変更。
- iOS 構成プロファイルのインストール。

デバイスが以下の状態のときにもパスコードが求められます。

- デバイスの電源を入れた直後、または再起動した直後。
- 48 時間以上デバイスのロックが解除されていない場合。
- デバイスのロック解除に過去 156 時間（6 日半）パスコードが使用されておらず、かつ過去 4 時間に生体認証でデバイスのロックを解除していない場合。
- デバイスがリモートのロックコマンドを受け取ったとき。
- 生体認証に 5 回失敗した後。
- 電源オフ／緊急 SOS 発信後。

Touch ID または Face ID が有効な場合、サイドボタンを押すとデバイスがすぐにロックされます。また、スリープ状態になったときも常にデバイスがロックされます。スリープを解除するには、Touch ID または Face ID で認証に成功するか、パスコードを入力する必要があります。

無作為に選ばれた他人が Touch ID で iPhone のロックを解除できる確率はおよそ 5 万分の 1、Face ID では 100 万分の 1 です。複数の指紋または顔を登録した場合は確率が上がり、5 つの指紋で最大 1 万分の 1、2 つの顔で最大 50 万分の 1 になります。さらに安全を強化するために、Touch ID と Face ID のどちらでも、認証に 5 回失敗したときはパスコードを入力しなければデバイスにアクセスできなくなります。Face ID での誤認率は、双子やよく似た兄弟姉妹の間では上がります。また、13 歳未満の子供同士でも、この年齢層では顔の特徴がまだ十分に定まっていないため、誤認率が上がります。この点に懸念がある場合は、認証にパスコードを使用することをお勧めします。

Touch ID のセキュリティ

Touch ID の指紋センサーは、ホームボタンを囲む静電容量式の金属リングが指の接触を検出したときにのみ起動します。指の接触が検出されると、高度なイメージングアレイが起動して指紋がスキャンされ、スキャン結果が Secure Enclave に送信されます。プロセッサと Touch ID センサー間の通信は、シリアル・ペリフェラル・インターフェイス経由で行われます。プロセッサは Secure Enclave にデータを渡すことはできますが、そのデータ自体を読み取ることはできません。通信はセッション鍵によって暗号化および認証されます。このセッション鍵は、製造時に各 Touch ID センサーとそれに対応する Secure Enclave に書き込まれた共有鍵を使ってネゴシエートされます。共有鍵は強力かつランダムで、Touch ID センサーごとに異なります。セッション鍵の交換には AES **鍵ラッピング**が使用されます。Touch ID センサーと Secure Enclave の両方がランダムな鍵を提供してセッション鍵を確立し、通信が AES-CCM によって暗号化されます。

ラスター形式のこのスキャン結果は、解析用にベクタ形式に変換されている間に Secure Enclave 内の暗号化されたメモリに一時的に保存され、その後破棄されます。解析は皮下の**隆線角度のマッピング**を利用して実行されます。これは不可逆的なプロセスで、ユーザの実際の指紋を再構築するために必要なマニューシャ（指紋の特徴点）のデータは破棄されます。結果として得られたノードのマップは、個人を特定する情報を含まず、暗号化された形式で保存され、Secure Enclave のみが読み出せます。このデータがデバイスの外に出ることはありません。Apple に送信されることも、デバイスのバックアップに含まれることもありません。

Face ID のセキュリティ

Face ID は、 ユーザが画面を注視していることを確認する誤認率の低い強力な認証技術で、 電子的または物理的どちらの手段でのなりすましも防ぐように設計されています。

ユーザが Face ID 対応 Apple デバイスを持ち上げるか画面をタップすることでスリープを解除する際や、 着信通知を表示するためにこれらのデバイスが認証を要求する際、 または対応する App が Face ID 認証を要求する際に、 TrueDepth カメラが自動的にユーザの顔を探します。 顔が検出されると、 ユーザがデバイスに顔を向け目を開けているかどうかが確認され、 その場合はユーザが画面を注視してロックを解除しようとしていると判断されます。 アクセシビリティ機能として、 VoiceOver が有効なときはこの確認が無効になります。 また、 必要に応じて別途無効にすることもできます。

ユーザが注視していることが確認されると、 TrueDepth カメラから 3 万以上の赤外線ドットが照射されて顔の形状が読み取られ、 顔の深度マップと 2D 赤外線イメージが生成されます。 このデータは、 2D イメージと深度マップのシーケンス生成に使用され、 デジタル署名されて Secure Enclave に送られます。電子的または物理的どちらの手段でのなりすましも防ぐために、 TrueDepth カメラによってキャプチャされた 2D イメージと深度マップのシーケンスがランダム化され、 デバイス固有のランダムパターンが生成されます。 Secure Enclave で保護されている A11 以降の SoC のニューラルエンジンの一部によって、 このデータが数学的モデルに変換され、 登録済みの顔認証データと比較されます。 登録済みの顔認証データも、 実体は、 さまざまな角度で撮影された顔のデータの数学的モデルです。

顔の照合は Secure Enclave 内で行われ、顔認証専用にトレーニングされたニューラルネットワークが使用されます。 顔の照合に使うニューラルネットワークの開発には、 参加者同意の下で実施された調査で収集した IR イメージおよび深度イメージを含む、 十億を超えるイメージが使用されています。 調査には、 性別、 年齢、 人種、 その他さまざまな要因を代表する世界中の人たちが参加しました。 さらに、 幅広いユーザの認識精度を向上させるために、 必要に応じて追加研究も実施されました。 Face ID では、 帽子、 スカーフ、 眼鏡、 コンタクトレンズ、 サングラスなどを身に付けていても顔を認識できます。 また、 屋内や屋外だけでなく、 完全な暗闇の中でも認識可能です。 一方で、 なりすましを見抜いて防止するためにトレーニングされた別のニューラルネットワークにより、 写真やマスクを使用して Face ID 対応 Apple デバイスのロックを解除しようとする試みは阻止されます。

ユーザの顔の数学的モデルを含む Face ID データは、 暗号化され、 Secure Enclave のみが使用できます。 このデータがデバイスの外に出ることはありません。 Apple に送信されることも、 デバイスのバックアップに含まれることもありません。 通常の操作時には、 以下の Face ID データが Secure Enclave で使用するためにのみ保存および暗号化されます。

- 登録時に計算された、 ユーザの顔の数学的モデル
- Face ID で認識精度の向上に有効だと判断されてロック解除時に計算された、 ユーザの顔の数学的モデル

通常の操作時に撮影した顔のイメージは保存されず、 Face ID データの登録のため、 または登録済みデータとの比較のために数学的モデルが計算されると、 ただちに破棄されます。

Touch ID または Face ID が iOS デバイスをロック解除する仕組み

Touch ID または Face ID が無効な場合は、 デバイスがロックされたときに、 Secure Enclave に保持されているデータ保護の最上位クラスの鍵が破棄されます。 このクラスのファイルおよび**キーチェーン**項目は、 ユーザがパスコードを入力してデバイスをロック解除しない限りアクセスできません。

Touch ID または Face ID が有効な場合は、 デバイスがロックされたときに鍵は破棄されず、 代わりに Secure Enclave 内の Touch ID または Face ID サブシステムに与えられている鍵でラップされます。 ユーザがデバイスをロック解除するときは、 認証に成功すると、 データ保護鍵をアンラップするための鍵が提供され、 デバイスがロック解除されます。 このプロセスでは、 デバイスをロック解除する際に、 データ保護と、 Touch ID または Face ID のサブシステムとの連携を必須にすることによって、 保護を強化しています。

デバイスを再起動すると、 Touch ID または Face ID でデバイスをロック解除するために必要な鍵は消去されます。 また、 パスコードの入力が必要な状況になったとき（48 時間以上ロック解除されなかったときや、 認証に 5 回失敗したときなど）は、 Secure Enclave によってこれらの鍵が破棄されます。

ロック解除のパフォーマンスを向上し、 ユーザの外見の自然な変化に対応するため、 Face ID では保存済みの数学的モデルが継続的に補強されます。 ロック解除に成功したときは、 その品質が十分であれば数学的モデルが新たに計算され、 Face ID で使用されることがあります。 この新しいデータは、 特定回数のロック解除後に破棄されます。 Face ID で顔認証に失敗した場合も、 そのマッチ率が特定のしきい値よりも高く、 直後にユーザがパスコードを入力して認証に成功したときは、 そのイメージから新しい数学的モデルが計算され、 登録済みの Face ID データが補強されます。 この新しい Face ID データは、 そのデータによる照合をユーザが中止した場合または特定回数のロック解除後に破棄されます。 こういった補強プロセスにより、 Face ID はユーザの髭や化粧による大きな変化に対応すると同時に、 誤認識を最小限に抑えます。

Touch ID、Face ID、Apple Pay

Touch ID または Face ID を Apple Pay で使用すると、 店舗、 App、 オンラインで簡単かつ安全に支払いができます。 Touch ID と Apple Pay については、 この文書の「Apple Pay」セクションを参照してください。

店舗での支払いを Face ID で認証する場合は、 まず、 サイドボタンをダブルクリックして支払いの意思を示す必要があります。 次に Face ID で認証を行ってから、 Face ID 対応 Apple デバイスを非接触型決済リーダーに近付けます。 Face ID で認証した後に Apple Pay での支払い方法を変更する場合は、 認証をやり直す必要があります。 ただし、 サイドボタンを再びダブルクリックする必要はありません。

App 内またはオンラインで Face ID を使って支払いをするときは、 サイドボタンをダブルクリックして支払いの意思を示してから、 Face ID で認証を行って支払いを承認します。 サイドボタンをダブルクリックしてから 30 秒以内に Apple Pay 決済が完了しなかった場合は、 もう一度サイドボタンをダブルクリックして支払いの意思を示す必要があります。

Face ID 診断

Face ID データは通常、 デバイスの外に出ることはなく、 iCloud やその他のどのバックアップにも含まれません。 ただし、 サポートを受けるためにユーザ自らが Face ID 診断データを AppleCare に提供することを決めた場合にのみ、 このデータがデバイスから転送されます。 Face ID 診断を使用するには、 ソフトウェア・アップデートのパーソナライズプロセスと同様に、 Apple からのデジタル署名による承認が必要です。 承認が完了すると、 Face ID 診断を有効にして、 Face ID 対応デバイスの「設定」 App から設定プロセスを開始できます。

Face ID 診断の設定中に、 既存の Face ID 登録データが削除され、 Face ID の再登録を求められます。 以後 10 日間、 Face ID 対応デバイスで認証時に記録された Face ID イメージが保存されます。 その期間が過ぎると、イメージの保存は自動的に停止します。 Face ID 診断では、 データが自動的に Apple に送信されることはありません。 診断モード中に収集された Face ID 診断データに含まれる登録イメージとロック解除時のイメージ（失敗と成功の両方）は、 ユーザが確認および承認した上で Apple に送信されます。 送信されるのはユーザが承認した Face ID 診断イメージのみです。 このデータは送信時に暗号化され、 送信後はただちにデバイスから削除されます。 送信を承認しなかったイメージはただちに削除されます。

イメージの確認や承認したイメージの送信を行わず、 Face ID 診断セッションが完了しなかった場合は、 40 日後に Face ID 診断が自動的に終了し、 すべての診断イメージがデバイスから削除されます。 また、 Face ID 診断はいつでも手動で無効にできます。 無効にすると、 デバイスに保存されたイメージがただちに削除されます。 上記いずれの場合も、 Face ID データが Apple に送信されることはありません。

Touch ID と Face ID のその他の用途

他社製 App では、システムが提供する API を使用して、Touch ID、Face ID、またはパスコードによる認証をユーザに求めることができます。Touch ID をサポートする App では、特別な変更なしに Face ID も自動的にサポートされます。Touch ID または Face ID の使用時は、App に認証の成否が通知されるだけで、App が Touch ID、Face ID、および登録ユーザに関連付けられたデータにアクセスすることはできません。キーチェーン項目を Touch ID または Face ID で保護して、そのいずれかまたはパスコードでの認証成功時にのみ Secure Enclave によってロック解除されるようにすることもできます。App のデベロッパは、キーチェーン項目をロック解除するために Touch ID、Face Id、またはパスコードを要求する前に、ユーザによってパスコードが設定されているかどうかを確認する API を使用します。App デベロッパは以下を行うことができます。

- 認証 API を使用する際に App のパスワードまたはデバイスのパスコードが再度要求されないようにできます。セキュリティが重視される App では、ユーザが登録されているかどうかを確認した上で、Touch ID または Face ID を第 2 要素として使用できます。
- Secure Enclave 内で ECC キーを生成して使用できます。これらは Touch ID または Face ID で保護されます。これらのキーを使用する処理は、常に Secure Enclave による承認の後、Secure Enclave 内で実行されます。

iTunes Store、App Store、および Apple Books での購入の承認に Touch ID または Face ID を使用することもできます。こうすることで、Apple ID パスワードの入力が不要になります。iOS 11 以降では、Touch ID または Face ID で保護された Secure Enclave ECC キーを使用することで、ストアからのリクエストに署名し、購入を承認します。

暗号化とデータ保護

すべてのコンテンツと設定を消去する

「設定」の「すべてのコンテンツと設定を消去」オプションでは、Effaceable Storage のすべての鍵が完全に消去され、デバイス上のすべてのユーザデータが暗号の仕組みによってアクセス不能になります。 そのため、デバイスをほかの人に譲渡したり修理に出したりする前にすべての個人情報をデバイスから確実に削除する場合に最適なオプションです。

重要：「すべてのコンテンツと設定を消去」を使用する前に、必ずデバイスをバックアップしてください。 消去されたデータはどのような方法でも復元することはできません。

セキュアブートチェーン、コード署名、およびランタイム・プロセス・セキュリティはすべて、信頼されたコードと App のみがデバイスで実行されることを保証するためのものです。 iOS にはこのほかにも暗号化とデータ保護の機能が搭載されており、セキュリティインフラストラクチャのほかの部分が危殆化した場合でも（たとえば不正に改ざんされたデバイスでも）、ユーザデータが保護されます。 これにより、個人や企業の情報が常時保護されるほか、デバイスの盗難または紛失時にも迅速かつ完全にリモートワイプを実行できる手段が提供されるため、ユーザと IT 管理者の双方が重要なメリットを得ることができます。

ハードウェアのセキュリティ機能

モバイルデバイスにおいては、スピードと電力効率が極めて重要です。 暗号演算は複雑であり、こうした優先事項を考慮せず設計および実装してしまうと、パフォーマンスやバッテリー駆動時間の問題が発生する場合があります。

すべての iOS デバイスには、フラッシュストレージとシステムのメインメモリ間の DMA パスに専用の AES-256 の暗号化エンジンが搭載されているので、ファイルの暗号化が非常に効率良く実行されます。 A9 以降の A シリーズプロセッサでは、フラッシュ・ストレージ・サブシステムは隔離されたバス上にあり、ユーザデータが含まれるメモリへのアクセスは DMA 暗号化エンジン経由でのみ許可されます。

デバイスの**ユニーク ID（UID）**とデバイス**グループ ID（GID）**は、製造時にアプリケーションプロセッサと Secure Enclave に焼き込まれた（UID の場合）または組み込まれた（GID の場合）AES-256 ビット鍵です。 ソフトウェアやファームウェアはそれらを直接読み出せず、シリコンに埋め込まれた専用の AES エンジンが UID または GID を鍵として実行した暗号化演算や復号演算の結果しか見ることができません。 アプリケーションプロセッサと Secure Enclave はそれぞれ独自の UID と GID を持ちます。 Secure Enclave の UID と GID は、Secure Enclave 専用の AES エンジンでしか使用できません。 UID と GID には、**Joint Test Action Group（JTAG）**などのデバッグインターフェイス経由でもアクセスすることはできません。

Apple A8 以前の SoC を除き、製造工程で Secure Enclave ごとに独自の UID（ユニーク ID）が生成されます。 UID は各デバイスに一意であり、また、デバイス外の製造システムではなく完全に Secure Enclave 内で生成されるため、この UID は Apple もサプライヤもアクセスできず、保存もされません。

Secure Enclave 上で実行されるソフトウェアは、デバイス固有の機密情報を保護するために UID を利用できます。 UID は暗号の仕組みを利用して、データを特定のデバイスに関連付けます。たとえば、ファイルシステムを保護する鍵階層には UID が含まれているので、メモリチップをあるデバイスから別のデバイスに物理的に移動した場合、そのファイルにはアクセスできなくなります。UID はデバイス上のその他の識別子には関連付けられていません。

GID はデバイスの特定クラス（たとえば Apple A8 プロセッサ搭載のすべてのデバイス）のすべてのプロセッサに共通です。

UID と GID 以外のその他すべての暗号鍵は、CTR_DRBG ソースコードに基づくアルゴリズムを使ってシステムの乱数ジェネレータ（RNG）により作成されます。 システムのエントロピーは、起動時のタイミングおよびデバイス起動完了後の割り込みタイミングから生成されます。 Secure Enclave 内で生成される鍵には、マルチリングオシレータで生成した後に CTR_DRBG で処理する真のハードウェア乱数ジェネレータが使用されます。

保存された鍵を安全に消去することは、鍵の生成と同様に重要です。たとえば、フラッシュストレージでは安全な消去が特に困難です。これは、フラッシュストレージのウェアレベリングのために、データの複数のコピーを消去する必要が生じる場合があるからです。この問題に対処するため、iOS デバイスには、**Effaceable Storage** というデータ消去専用の安全な機能が搭載されています。この機能は、下層のストレージテクノロジー（NAND など）にアクセスして、ごく下位にあるわずかなブロックを直接操作して消去します。

予備電力機能付きエクスプレスカード

iPhone のバッテリー残量がわずかになって iOS が動作していない状態でも、残りの電力でエクスプレスカードを処理できる場合があります。

この機能をサポートする iPhone モデルでは、次のカードでこの機能が自動的に有効になります。

- エクスプレスカードとして指定された交通系 IC カード
- エクスプレスモードがオンになっている学生証

サイドボタンを押すと、バッテリー残量低下アイコンと共に、エクスプレスカードを使用できることを示すテキストが表示されます。iOS の正常動作時と同じ条件下で、NFC コントローラによってエクスプレスカードの処理が実行されます。ただし、実行されたことは触覚による通知でのみ知らされ、画面には表示されません。

この機能は、ユーザが手動でシャットダウンを行った場合には使用できません。

ファイルのデータ保護

Apple は、iOS デバイスに内蔵されているハードウェア暗号化機能に加えて、データ保護という技術を採用して、デバイスのフラッシュメモリに保存されるデータの保護を強化しています。データ保護により、デバイスで電話の着信などの一般的なイベントに応答するだけでなく、ユーザデータを高いレベルで暗号化することが可能になっています。「メッセージ」、「メール」、「カレンダー」、「連絡先」、「写真」、および「ヘルスケア」などの重要なシステム App のデータ値では、デフォルトでデータ保護が使用されます。iOS 7 以降にインストールされた他社製 App は、自動的にこのデータ保護が適用されます。

データ保護は、鍵の階層を構築して管理することで実装され、すべての iOS デバイスに内蔵されたハードウェア暗号化テクノロジーをベースにしています。データ保護は、各ファイルをクラスに割り当てることでファイルごとに制御されます。ファイルにアクセスできるかどうかは、そのクラスキーがロック解除されているかどうかによって決定されます。さらに、Apple File System（APFS）の登場により、鍵をエクステントごとにさらに分割できる（ファイルの一部に別の鍵を持たせることができる）ようになっています。

アーキテクチャの概要

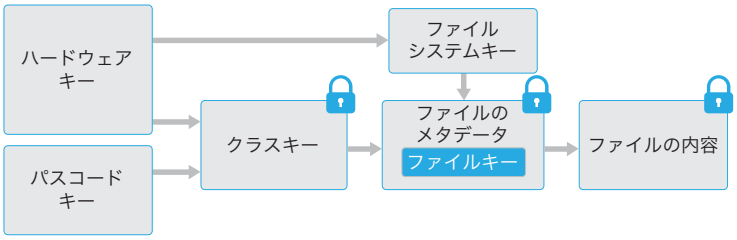
データパーティション上にファイルが作成されるたびに、データ保護によって新しい 256 ビット鍵（「Per File」キー）が作成され、ハードウェア AES エンジンに渡されます。そしてハードウェア AES エンジンによりその鍵が使われ、ファイルがフラッシュメモリに書き込まれるときに AES-XTS モードでファイルが暗号化されます。A7、S2、または S3 SoC を搭載したデバイスでは、AES-CBC モードが使用されます。初期化ベクトルはファイルのブロックオフセットを使って計算され、**Per File キー**の SHA-1 ハッシュを使用して暗号化されます。

Per File（または Per Extent）キーは複数あるクラスキーのうちのいずれかでラップされます。このときのクラスキーは、ファイルへのアクセス条件によって異なります。その他すべての鍵ラッピングと同様に、これも RFC 3394 に基づく NIST AES 鍵ラッピングで実行されます。ラップされた Per File キーは、ファイルのメタデータに保存されます。

Apple File System を使用するデバイスでは、 ファイルのクローン作成 （コピーオンライト技術を使用したゼロコストコピー） がサポートされることがあります。 ファイルのクローンを作成すると、それぞれのクローンごとに書き込み入力を受け付けるための新しい鍵が生成されます。 新しいデータは、 新しい鍵を使用してメディアに書き込まれます。 時間の経過により、 ファイルがさまざまなエクステント （断片） で構成され、 そのそれぞれが異なる鍵に対応付けられるようになることがあります。 ただし、 1 つのファイルを構成するすべてのエクステントは、 同じクラスキーによって保護されます。

ファイルが開かれると、 そのファイルのメタデータが**ファイルシステムキー**で復号され、 ラップされた Per File キーとファイルを保護しているクラスの方式が明らかになります。 Per File （または Per Extent） キーは、 クラスキーによってアンラップされてから、 ハードウェア AES エンジンに渡されます。 そしてフラッシュメモリからファイルを読み出すときに、 ハードウェア AES エンジンがファイルを復号します。 ラップされたファイルキーの処理はすべて Secure Enclave 内で実行されます。 そのため、 ファイルキーがアプリケーションプロセッサに直接公開されることはありません。 起動時に、 Secure Enclave は AES エンジンと一時鍵のネゴシエーションを行います。 Secure Enclave がファイルの鍵をアンラップした場合、 その鍵は一時鍵で再度ラップされてからアプリケーションプロセッサに戻されます。

ファイルシステム内のすべてのファイルのメタデータは、ランダムな鍵で暗号化されます。 この鍵は、iOS がはじめてインストールされたとき、 またはユーザによってデバイスがワイプされたときに作成されます。 Apple File System をサポートするデバイスでは、ファイルシステムのメタデータキーが、 長期保存のために Secure Enclave UID キーによってラップされます。 Per File または Per Extent キーと同様に、 メタデータキーもアプリケーションプロセッサに直接公開されることはありません。 代わりに、 起動のたびに Secure Enclave によって一時鍵が提供されます。 暗号化されたファイルシステムキーは、 保存時に、 Effaceable Storage に保存された「消去可能な鍵」 によってさらにラップされます。 この鍵は、 データの機密性を高めるために使用されるのではなく、 要求に応じてすばやく消去されるように設計されています （ユーザが「すべてのコンテンツと設定を消去」 オプションを選択するか、 ユーザまたは管理者が MDM ソリューション、Exchange ActiveSync、 または iCloud からリモート・ワイプ・コマンドを発行すると消去されます）。 このようにして鍵を消去すると、 すべてのファイルが暗号の仕組みによってアクセス不可になります。



ファイルの内容は 1 つまたは複数の Per File （または Per Extent） キーで暗号化されることがあります。 これらのキーはクラスキーでラップされてファイルのメタデータに保存されます。 そしてメタデータはファイルシステムキーで暗号化されます。 クラスキーはハードウェア UID で保護されますが、 ユーザのパスコードで保護されるクラスもあります。 このような階層構造により、 柔軟性とパフォーマンスの両方を実現しています。 たとえば、 ファイルのクラスを変更する場合はそのファイルの Per File キーをラップし直すだけでよく、 パスコードを変更した場合はクラスキーのラップだけが変更されます。

パスコード

デバイスパスコードを設定することで、 ユーザはデータ保護を自動的に有効にできます。 iOS は、6 桁の数字、 4 桁の数字、 および英数字を含む任意の長さのパスコードをサポートしています。 パスコードを設定すると、 デバイスをロック解除するだけでなく、 一部の暗号鍵にエントロピーを付加することができます。 これによって、 デバイスを乗っ取った攻撃者は、 パスコードがない限り特定の保護クラスのデータにアクセスできなくなります。

パスコードの検討事項

数字のみを含む長いパスワードを入力する場合は、ロック画面にフルキーボードではなくテンキーが表示されます。 数字のみの長いパスコードは英数字を含む短いパスコードよりも簡単に入力できますが、同水準のセキュリティを確保できます。

パスコードはデバイスの UID とタングルされる（関連付けられる）ので、総当たり（ブルートフォース）攻撃を行うには対象のデバイス上で実行する必要があります。 各試行にかかる時間を長くするために、 反復間隔が大きく設定されています。 反復間隔は、 試行 1 回につき約 80 ミリ秒かかるように調整されているので、 英数字 6 文字のパスコードの場合、 すべての組み合わせを試すには 5 年半以上かかることになります。

パスコード入力間の待ち時間

入力回数	強制される待ち時間
1 ～ 4	なし
5	1 分
6	5 分
7 ～ 8	15 分
9	1 時間

ユーザパスコードが強力であれば、 それだけ暗号鍵も強力になります。 Touch ID や Face ID を使用すれば、 これらを使用しない場合は実用的ではない長さのパスコードも設定しやすくなるので、 その分暗号鍵も強化されます。 これにより、 1 日に何度も実行する iOS デバイスのロック解除のユーザ体験を損なうことなく、 データ保護用の暗号鍵を保護するエントロピーの有効性を増大させることができます。

パスコードに対する総当たり（ブルートフォース）攻撃をさらに抑制するために、 ロック画面で無効なパスコードが入力された場合、次の入力までの待ち時間が延長されます。「設定」 >「Face ID とパスコード」 >「データを消去」がオンの場合、 パスコードの入力を 10 回連続で間違えるとデバイスが自動的にワイプされます。 同じ内容の間違ったパスコードを連続で入力した場合はカウントされません。 この設定は、 この機能をサポートする MDM ソリューションおよび Exchange ActiveSync の管理ポリシーとしても利用可能で、 回数の上限を下げることもできます。

Secure Enclave を搭載したデバイスでは、 Secure Enclave コプロセッサによって待ち時間が強制的に適用されます。 遅延が適用されているデバイスを再起動しても遅延は適用されたまま、再起動前のカウントが再開されます。

使いやすさを維持しながらセキュリティを高めるため、 iOS 11.4.1 以降では、 USB をしばらく使用しなかった場合、 USB インターフェイスをアクティブにするために Touch ID、 Face ID、またはコードの入力が必要になります。 これにより、 マルウェアが仕込まれた充電器など、 物理的に接続するデバイスに対して攻撃領域を狭めながら、 適度な時間的制約内で USB アクセサリの使いやすさも保てるようになります。 iOS デバイスのロック後または USB 接続の解除後 1 時間以上経つと、 デバイスのロックを解除するまで、 新たな接続は一切確立できなくなります。 この 1 時間という制限には次の利点があります。

- Mac、 PC、 USB アクセサリとの接続、 または CarPlay との有線接続を頻繁に行う場合は、デバイスを接続するたびにパスコードを入力する必要がない。
- USB アクセサリのエコシステムでは、 データ接続の確立前にアクセサリを識別する確実な方法が提供されていないため、 それを補うことができる。

さらに iOS 12 では、USB 接続が確立されてから 3 日以上経過している場合と、デバイスをロックした後、 ただちに新たな USB 接続を確立できなくなります。 これにより、 USB 接続をあまり使用しないユーザへのセキュリティが向上します。 また、生体認証を再度有効にするためにパスコードが必要な状態のときにも、 USB 接続が無効になります。

ユーザは、「設定」で USB 接続を常時オンにするように選択できます。 また、 一部の操作支援デバイスでは設定時に常時オンが自動的に選択されます。

DFU モードとリカバリモード

Apple A10、 A11、 または S3 SoC を搭載したデバイスでは、 リカバリモードにおいてユーザのパスコードで保護されたクラスキーはアクセス不能となります。 A12 または S4 SoC では、この保護が DFU モードにも適用されます。

Secure Enclave の AES エンジンには、 ロック可能なソフトウェア・シード・ビットが実装されています。 UID から鍵が生成されると、 追加の鍵階層を構築するために、 鍵派生関数にこれらのシードビットが埋め込まれます。

Apple A10 または S3 以降の SoC では、 ユーザのパスコードによって保護される鍵を識別するために 1 つのシードビットが専用で使用されます。 このシードビットは、 ユーザのパスコードが必要な鍵（データ保護クラス A、 クラス B、 クラス C 鍵など）では設定され、 ユーザのパスコードが不要な鍵（ファイルシステムメタデータキー、 クラス D 鍵など）では設定されません。

A12 SoC では、アプリケーションプロセッサが DFU モードまたはリカバリモードに入ると、Secure Enclave Boot ROM によってパスコードのシードビットがロックされます。パスコードのシードビットがロックされているときは、ビットを変更する操作が禁止されるため、ユーザのパスコードで保護されたデータへのアクセスを防ぐことができます。

Apple A10、A11、S3、または S4 SoC では、デバイスがリカバリモードに入ると、Secure Enclave OS によってパスコードのシードビットがロックされます。Secure Enclave Boot ROM と Secure Enclave OS は、どちらも、ブート・プログレス・レジスタをチェックすることによって現在のモードを安全に判断します。

データ保護クラス

iOS デバイス上に新しいファイルが作成されると、ファイルを作成した App によってクラスが割り当てられます。データへのアクセス条件を決定するポリシーはクラスごとに異なります。基本のクラスとポリシーについて、以下のセクションで説明します。

Complete Protection

（`NSFileProtectionComplete`）：クラスキーは、ユーザのパスコードとデバイスの UID から生成される鍵によって保護されます。ユーザがデバイスをロックした直後（「パスコードを要求」が「即時」に設定されている場合は 10 秒）、復号されたクラスキーが破棄され、このクラスのすべてのデータは、ユーザがパスコードを再度入力するか Touch ID または Face ID でデバイスをロック解除しない限りアクセスできなくなります。

Protected Unless Open

（`NSFileProtectionCompleteUnlessOpen`）：ファイルの中には、デバイスのロック中に書き込みが必要なものもあります。バックグラウンドでダウンロードされるメールの添付ファイルが良い例です。この動作は、楕円曲線に基づく非対称暗号方式（Curve25519 を使用する ECDH）により可能になっています。通常の Per File キーは、NIST SP 800-56A に記述された One-Pass Diffie-Hellman Key Agreement を使って保護されます。

この鍵共有に使用する一時公開鍵は、ラップされた Per File キーと共に保存されます。鍵派生関数は、NIST SP 800-56A の 5.8.1 に記述された Concatenation Key Derivation Function（Approved Alternative 1）です。AlgorithmID は省略されています。PartyUInfo と PartyVInfo はそれぞれ一時的な公開鍵と静的な公開鍵です。SHA-256 がハッシュ関数として使用されます。ファイルが閉じられると、Per File キーはすぐにメモリからワイプされます。再度ファイルを開く場合は、Protected Unless Open クラスの秘密鍵とファイルの一時公開鍵を使って共有秘密鍵が再度作成されます。これらは Per File キーをアンラップするために使用され、Per File キーはファイルの復号に使用されます。

Protected Until First User Authentication

（`NSFileProtectionCompleteUntilFirstUserAuthentication`）：このクラスは Complete Protection と同じように動作します。ただし、復号されたクラスキーは、デバイスのロック時にメモリから削除されません。このクラスの保護は、デスクトップ環境でのボリューム全体の暗号化と似ており、デバイスを再起動させる攻撃からデータを保護します。すべての他社製 App では、データをほかのデータ保護クラスに割り当てない限り、これがデータのデフォルトクラスになります。

No Protection

（`NSFileProtectionNone`）：このクラスキーは UID でのみ保護され、Effaceable Storage に保存されます。このクラスのファイルの復号に必要な鍵はすべてデバイスに保存されるため、この暗号化から得られるメリットは、迅速なリモートワイプができるということだけです。ファイルにデータ保護クラスが割り当てられていない場合でも、iOS デバイス上のすべてのデータと同様にファイルは暗号化された形式で保存されます。

データ保護クラスキー

Class A Complete Protection	(NSFileProtectionComplete)
Class B Protected Unless Open	(NSFileProtectionCompleteUnlessOpen)
Class C Protected Until First User Authentication	(NSFileProtectionCompleteUntilFirstUserAuthentication)
Class D No Protection	(NSFileProtectionNone)

キーチェーンのデータ保護

多くの App はパスワードだけでなく、その他の短くも機密性の高いデータ片（鍵やログイントークンなど）を扱う必要があります。iOS キーチェーンには、これらの項目を安全に保存する方法が用意されています。

キーチェーン項目は、表のキー（メタデータ）と行ごとのキー（秘密鍵）という 2 つの異なる AES-256-GCM 鍵を使用して暗号化されます。キーチェーンのメタデータ（kSecValue 以外のすべての属性）は検索速度を高めるためにメタデータキーで暗号化され、秘密値（kSecValueData）は別の秘密鍵で暗号化されます。メタデータキーは Secure Enclave プロセッサによって保護されますが、キーチェーンの照会を高速化するためにアプリケーションプロセッサにキャッシュされます。秘密鍵は常に、Secure Enclave プロセッサを介してやりとりする必要があります。

キーチェーンは SQLite データベース形式で実装され、ファイルシステムに保存されています。データベースは 1 つしかなく、各プロセスや App がアクセスできるキーチェーン項目は、**securityd** デーモンによって決定されます。キーチェーンアクセス API によりデーモンが呼び出され、このデーモンによって App の「Keychain-access-groups」、「application-identifier」、および「application-group」の各エンタイトルメントが照会されます。アクセスは 1 つのプロセスには限定されないので、アクセスグループを利用してキーチェーン項目を App 間で共有することができます。

キーチェーン項目の共有は、同じデベロッパによる App 間でのみ可能です。この仕組みは、Apple Developer Program のアプリケーショングループを通じて割り当てられたプレフィックスに基づくアクセスグループの使用を他社製 App に義務付けることで管理されています。プレフィックス要件とアプリケーショングループの一意性は、コード署名、**プロビジョニングプロファイル**、および Apple Developer Program によって実現されます。

キーチェーンデータは、ファイルのデータ保護で使用されるものと同様のクラス構造で保護されます。これらのクラスは、ファイルのデータ保護の各クラスと同じように動作します。ただし、固有の鍵が使用され、API の名前も異なります。

利用できるタイミング	ファイルのデータ保護	キーチェーンデータ保護
ロック解除時	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
ロック中	NSFileProtectionCompleteUnlessOpen	不可
初回ロック解除後	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
常時	NSFileProtectionNone	kSecAttrAccessibleAlways
パスコードが有効なとき	不可	kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

バックグラウンド更新サービスを利用する App は、バックグラウンドでのアップデート中にアクセスする必要があるキーチェーン項目に `kSecAttrAccessibleAfterFirstUnlock` を使用できます。

キーチェーン項目のコンポーネント

アクセスグループのほかに、各キーチェーン項目には管理メタデータ（「作成日」や「前回のアップデート」のタイムスタンプなど）が含まれます。

また、項目（アカウントやサーバ名など）を照会するための属性の SHA-1 ハッシュも含まれているので、各項目を復号せずに検索することができます。さらに、以下を含む暗号化データも含まれています。

- バージョン番号
- アクセス制御リスト（ACL）データ
- 項目が属する保護クラスを示す値
- 保護クラスキーでラップされた Per Item キー
- バイナリ形式の plist にエンコードされ Per Item キーで暗号化された、項目を説明する属性辞書（SecItemAdd に渡されます）

暗号化方式は、AES-256 GCM（Galois/Counter Mode）です。アクセスグループは属性に含まれ、暗号化中に計算される GMAC タグで保護されます。

クラス `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly` の動作は `kSecAttrAccessibleWhenUnlocked` と同じですが、 利用できるのはデバイスにパスコードが構成されているときのみです。 このクラスはシステム**キーバッグ**にのみ存在し、 以下の特徴があります。

- iCloud キーチェーンに同期されない
- バックアップされない
- エスクローキーバッグに含まれない

パスコードが削除またはリセットされた場合、 クラスキーが破棄されることによって、 これらの項目は使用できなくなります。

その他のキーチェーンクラスにも「このデバイスのみ」 に該当する保護クラスがあります。 このクラスはバックアップ中にデバイスからコピーされるときに UID で常時保護されるので、 別のデバイスに復元されると使用できなくなります。 Apple は、 保護する情報の種類や iOS で必要になるタイミングに応じてキーチェーンクラスを選択することで、 セキュリティと使いやすさのバランスに配慮しています。 たとえば、 デバイスをいつでも VPN 接続可能にするために、 VPN 証明書は常に利用できる状態になっている必要がありますが、「移行不可」 に分類されているので別のデバイスに移動することはできません。

iOS で作成されたキーチェーン項目については、 以下のクラス保護が強制的に適用されます。

項目	アクセスできるタイミング
Wi-Fi パスワード	初回ロック解除後
メールアカウント	初回ロック解除後
Exchange アカウント	初回ロック解除後
VPN パスワード	初回ロック解除後
LDAP、 CalDAV、 CardDAV	初回ロック解除後
ソーシャル・ネットワーク・アカウントのトークン	初回ロック解除後
Handoff アドバタイズメント暗号化鍵	初回ロック解除後
iCloud トークン	初回ロック解除後
ホームシェアリングパスワード	ロック解除時
「iPhone を探す」 トークン	常時
留守番電話	常時
iTunes バックアップ	ロック解除時、 移行不可
Safari パスワード	ロック解除時
Safari ブックマーク	ロック解除時
VPN 証明書	常時、 移行不可
Bluetooth® 鍵	常時、 移行不可
Apple Push Notification service トークン	常時、 移行不可
iCloud の証明書と秘密鍵	常時、 移行不可
iMessage 鍵	常時、 移行不可
構成プロファイルによってインストールされる証明書と秘密鍵	常時、 移行不可
SIM PIN	常時、 移行不可

キーチェーンアクセス制御

キーチェーンでは、 アクセス制御リスト （ACL） を使用して、 アクセス権や認証要件のポリシーを設定できます。 Touch ID や Face ID の使用またはデバイスのパスコードの入力による認証がない限り項目にアクセスできないように設定することで、 正当なユーザが実際にデバイスを使用しているという条件を項目に設けることができます。 また、 項目の追加後に Touch ID または Face ID の登録が変更されていないという条件を指定して、 項目へのアクセスを制限することもできます。 この

制限により、攻撃者が自分の指紋を追加してキーチェーン項目にアクセスすることを防止できます。ACL は Secure Enclave 内で評価され、指定した制限が満たされた場合にのみカーネルに渡されます。

キーバッグ

ファイルとキーチェーンのデータ保護クラスの鍵は、キーバッグに収集されて管理されます。iOS では、ユーザ、デバイス、バックアップ、エスクロー、iCloud バックアップのキーバッグが使用されます。

ユーザキーバッグには、デバイスの通常の操作に使用されるクラスキーがラップされて保存されています。たとえば、パスコードが入力されると、`NSFileProtectionComplete` キーがユーザキーバッグから読み込まれ、アンラップされます。これは No Protection クラスに保存されているバイナリ形式のプロパティリスト（.plist）ファイルで、その内容は Effaceable Storage に保存されている鍵で暗号化されています。キーバッグに前方秘匿性を追加するために、この鍵はユーザがパスコードを変更するたびにワイプされ再生成されます。`AppleKeyStore` カーネル機能拡張はユーザキーバッグを管理しており、デバイスのロック状態に関してはこのカーネル機能拡張に照会できます。ユーザキーバッグ内のすべてのクラスキーがアクセスできる状態になっていて、正しくアンラップされている場合にのみ、AppleKeyStore はデバイスがロック解除されていると報告します。

デバイスキーバッグは、デバイス固有のデータを扱う操作で使用するクラスキーのラップと保存に使用されます。共有して使用できるよう構成されている iOS デバイスでは、ユーザのログイン前に資格情報へのアクセスが必要な場合があるため、ユーザのパスコードで保護されていないキーバッグが必要になります。iOS は、ユーザごとに分離したファイルシステムコンテンツの暗号化をサポートしないため、システムはデバイスキーバッグのクラスキーを使用して Per File キーをラップすることになります。ただし、キーチェーンはユーザキーバッグからのクラスキーを使用して、ユーザキーチェーン内の項目を保護します。単一ユーザが使用するように構成されている iOS デバイス（デフォルト構成）では、デバイスキーバッグとユーザキーバッグは同じものとなり、これはユーザのパスコードによって保護されます。

バックアップキーバッグは、「iTunes」による暗号化されたバックアップが行われたときに作成され、デバイスのバックアップ先となるコンピュータに保存されます。新しいキーバッグには新しい鍵のセットも作成され、バックアップデータはこれらの新しい鍵で再度暗号化されます。前述の通り、移行不可のキーチェーン項目は UID 由来の鍵でラップされたままになっているため、これらはオリジナルのバックアップ元のデバイスには復元できますが、別のデバイスに復元した場合はアクセスできなくなります。

バックアップキーバッグは「iTunes」で設定されたパスワードで保護され、PBKDF2 が 1000 万回反復実行されます。反復回数はこれだけ多く設定されていますが、特定のデバイスには関連付けられません。そのため理論上は、バックアップキーバッグは多数のコンピュータから同時並行的に総当たり（ブルートフォース）攻撃される可能性があります。こうした脅威は、十分に強いパスワードを使用することで軽減できます。

ユーザが iTunes バックアップを暗号化しない場合は、データ保護クラスにかかわらずバックアップファイルは暗号化されません。ただし、この場合でもキーチェーンは UID 由来の鍵で保護されます。このため、キーチェーン項目を新しいデバイスに移行できるのは、バックアップパスワードが設定されている場合のみです。

エスクローキーバッグは、「iTunes」の同期とモバイルデバイス管理（MDM）に使用されます。このキーバッグにより、「iTunes」がバックアップや同期をするときにユーザによるパスコードの入力が不要になるほか、MDM ソリューションがユーザのパスコードをリモートで消去することが可能になります。エスクローキーバッグは、「iTunes」との同期に使用されるコンピュータか、デバイスをリモート管理する MDM ソリューションに保存されます。

エスクローキーバッグにより、すべてのクラスのデータへのアクセスが必要になる場合があるデバイス同期でのユーザ体験が向上します。パスコードでロックされたデバイスがはじめて「iTunes」に接続されると、ユーザはパスコードの入力を求められます。その後、デバイスで使用されているものと同じクラスキーを含むエスクローキーバッグがデバイスによって作成されます。エスクローキーバッグは、新たに生成された鍵で保護されます。エスクローキーバッグとそれを保護する鍵は、デバイスとホストまたはデバイスとサーバに分けて保存され、デバイスに保存されているデータには Protected Until First User Authentication クラスが割り当てられます。このため、デバイスの再起動後にはじめて「iTunes」でバックアップを作成するときに、デバイスのパスコードの入力が必要になります。

ワイヤレス（OTA）でのソフトウェア・アップデートの場合、ユーザはアップデート開始時にパスコードの入力を求められます。このパスコードを使用して、アップデート後にユーザキーバッグをロック解除するためのワンタイムロック解除トークンが安全に作成されます。このトークンは、ユーザのパスコードを入力しないと生成できません。また、ユーザのパスコードが変更された場合、以前に生成されたトークンはすべて無効になります。

ワンタイムロック解除トークンは、ソフトウェア・アップデートの手動インストールおよび自動インストールの両方で使用されます。このトークンは、Secure Enclave のモノトニックカウンタの現在値、キーバッグの UUID、および Secure Enclave の UID から派生した鍵で暗号化されます。

Secure Enclave 内のワンタイムロック解除トークンのカウンタが増分されると、既存のトークンがすべて無効になります。カウンタが増分されるのは、トークンが使用されたとき、再起動したデバイスの初回のロック解除後ソフトウェア・アップデートがユーザまたはシステムによってキャンセルされたとき、またはトークンのポリシータイマーが期限切れになったときです。

手動ソフトウェア・アップデートのワンタイムロック解除トークンは 20 分後に無効になります。このトークンは Secure Enclave から書き出され、Effaceable Storage に書き込まれます。デバイスが 20 分以内に再起動しなかった場合、ポリシータイマーによってカウンタが増分されます。

自動ソフトウェア・アップデートは、入手可能なアップデートが検出され、以下のいずれかの条件を満たしたときに実行されます。

- iOS 12 で自動アップデートが設定されている。
- アップデートの通知時にユーザが「あとでインストール」を選択した。

ユーザがパスコードを入力すると、ワンタイムロック解除トークンが生成され、Secure Enclave 内で最大 8 時間有効な状態になります。アップデートが実行されない限り、このワンタイムロック解除トークンは、ロックするたびに破棄され、次のロック解除時に再作成されます。また、ロック解除のたびに 8 時間の有効期間が再開されます。

8 時間が経過すると、ポリシータイマーによってワンタイムロック解除トークンが無効にされます。

iCloud バックアップキーバッグは、バックアップキーバッグに似ています。このキーバッグ内のすべてのクラスキーは非対称鍵（Protected Unless Open データ保護クラスと同様に Curve25519 を使用）なので、iCloud バックアップはバックグラウンドで実行することができます。No Protection 以外のすべてのデータ保護クラスでは、暗号化されたデータがデバイスから読み出されて iCloud に送信されます。対応するクラスキーは iCloud キーによって保護されます。キーチェーンクラスキーは、暗号化されていない iTunes バックアップと同様に、UID 由来の鍵でラップされます。iCloud キーチェーンのキーチェーン復元でのバックアップにも非対称キーバッグが使用されます。

App のセキュリティ

App は現代のモバイル・セキュリティ・アーキテクチャにおいて最も重要な要素の 1 つです。App は生産性においてすばらしいメリットをもたらす一方で、適切に扱わないと、システムのセキュリティ、安定性、およびユーザデータに悪影響を及ぼす可能性があります。

このため、iOS では複数の保護レイヤーを構築し、App が署名され、検証され、サンドボックス化されていることを保証することでユーザデータを保護しています。これらの要素によって安定した安全な App プラットフォームが提供されているので、何千人ものデベロッパによる数十万もの App を、システムの完全性を損なうことなく iOS に配信することが可能になっています。それにより、ユーザも、ウイルス、マルウェア、不正な攻撃などを過度に心配することなく、iOS デバイス上のこれらの App に安心してアクセスできるようになります。

App のコード署名

iOS のカーネルが起動すると、どのユーザプロセスと App の実行を許可するかをカーネルが制御します。すべての App が既知の承認済みのソースから提供されており、改ざんされていないことを保証するため、iOS では、すべての実行コードに対して、Apple 発行の証明書を使用した署名を要求しています。「メール」や「Safari」といったデバイスに付属する App は、Apple によって署名されています。他社製 App も、Apple 発行の証明書を使用して検証および署名される必要があります。こうしたコード署名を強制することで、信頼チェーンの概念を OS から App へと延長することができ、他社製 App によって未署名のコードリソースが読み込まれたり、自己書き換えコードが使用されたりするのを防ぐことができます。

App を開発して iOS デバイスにインストールするには、デベロッパは Apple に登録し、Apple Developer Program に参加する必要があります。個人または企業のいずれの場合でも、Apple がデベロッパの身元確認を行った後に証明書が発行されます。この証明書によって、デベロッパは App に署名し、App を App Store に提出して配信できるようになります。したがって、App Store にあるすべての App は、身元を確認できる個人または組織によって提出されたものであり、これは悪意のある App 開発に対する抑止力にもなります。また、Apple は、App が説明の通りに動作し、明らかなバグや何らかの問題が含まれていないことを確認するための審査も行います。前述のセキュリティ技術に加え、このような選別プロセスを実施することで、ユーザは App の品質について懸念することなく安心して購入できるようになります。

iOS では、デベロッパが App 内にフレームワークを埋め込み、そのフレームワークを App 自体または App に埋め込まれた機能拡張で使用することが可能です。システムやその他の App がそのアドレス空間内に第三者のコードを読み込むことを防止するため、プロセスがリンクするすべてのダイナミックライブラリについて、起動時にコード署名の検証が実行されます。この検証は、Apple 発行の証明書から抽出されるチーム識別子（チーム ID）を使って実施されます。チーム識別子は、英数字 10 文字（例：1A2B3C4D5F）で構成されます。プログラムは、システムに付属のプラットフォームライブラリや、コード署名内にメインの実行可能ファイルと同じチーム識別子を持つライブラリにリンクできます。システムの一部として提供される実行可能ファイルにはチーム識別子が含まれていないため、これらの実行可能ファイルはシステム自体に付属のライブラリにのみリンクできます。

企業は組織内で使用するための社内 App を開発して、従業員に配付することもできます。企業や組織は D-U-N-S 番号を使って Apple Developer Enterprise Program（ADEP）に申請できます。Apple は身元と登録資格を確認してから申請を承認します。組織が ADEP に登録されると、承認したデバイスで社内 App の実行を許可するプロビジョニングプロファイルを登録して取得できます。ユーザが社内 App を実行するには、プロビジョニングプロファイルをインストールする必要があります。このため、組織が意図したユーザしか、組織の App を iOS デバイスに読み込めません。MDM でインストールされた App は、組織とデバイス間の信頼関係がすでに

確立されているため、暗黙的に信頼されます。それ以外の App については、ユーザが「設定」で App のプロビジョニングプロファイルを承認する必要があります。組織は、不明なデベロッパの App をユーザが承認しないように制限できます。どのエンタープライズ App でも、初回起動時に App の実行を許可するという Apple からの許諾をデバイスで受信する必要があります。

ほかのモバイルプラットフォームとは異なり、iOS では、ユーザは悪意のある可能性のある未署名の App を Web サイトからインストールしたり、信頼されていないコードを実行したりすることはできません。実行時には、実行可能ファイルのメモリページが読み込まれるときに、そのすべてについてコード署名チェックが実行され、インストールまたは前回のアップデート以降に App が改変されていないことが確認されます。

ランタイム・プロセス・セキュリティ

App が承認済みのソースからのものであることが確認されると、ほかの App やシステムのほかの部分の危殆化を防止するための iOS のセキュリティ対策が強制的に適用されます。

他社製 App はすべて「サンドボックス化」されるので、ほかの App によって保存されたファイルにアクセスしたり、デバイスに変更を加えたりすることはできません。これにより、ほかの App によって保存された情報が収集または変更されるのを防ぐことができます。各 App にはファイルを保存する専用のホームディレクトリが用意されますが、これは App がインストールされるときにランダムに割り当てられます。他社製 App が自身の情報以外の情報にアクセスする必要がある場合は、iOS によって明示的に提供されるサービスを使用したときのみアクセスできます。

システムファイルとリソースもユーザの App から保護されます。iOS の大部分は、他社製 App と同様に特権のないユーザ「mobile」として実行されます。OS のパーティション全体は、読み出し専用としてマウントされます。リモート・ログイン・サービスなどの不要なツールは、システムソフトウェアには含まれていません。また、App が API を使って自身の権限を昇格させてほかの App や iOS 自体を変更することもできません。

他社製 App によるユーザ情報や iCloud のような機能や拡張性へのアクセスは、宣言されたエンタイトルメントにより制御されます。エンタイトルメントは、App に含まれる署名されたキー値ペアで、UNIX ユーザ ID のようなランタイム要素以外の認証を可能にします。エンタイトルメントはデジタル署名されているため変更できません。エンタイトルメントは、システムアプリケーションやデーモンが特権を必要とする特定の操作を実行するために頻繁に使用されます。エンタイトルメントがないと、プロセスをルートで実行しなければなりません。この機能により、不正なシステム App やデーモンによる権限昇格のリスクを大幅に低減できます。

さらに、App はシステムが提供する API 経由でしかバックグラウンド処理を実行できません。これにより、App はパフォーマンスを低下させたりバッテリー駆動時間を大きく損ねたりすることなく、機能し続けることができます。

アドレス空間配置のランダム化（ASLR）は、メモリ破壊バグの悪用を防止します。内蔵 App は、ASLR を使用して、起動時にすべてのメモリ領域がランダム化されることを確認します。さらに、実行コード、システムライブラリ、および関連するプログラミング構成体のメモリアドレスがランダムに配置されるので、多くの高度な攻撃が発生する可能性も低減します。たとえば、「return-to-libc」攻撃は、スタックとシステムライブラリのメモリアドレスを操作することで、デバイスに悪意のあるコードを実行させようとします。これらのメモリアドレスのランダムに配置することにより、その攻撃の実行が格段に難しくなります。特に複数のデバイスを標的とする攻撃は極めて困難になります。iOS の開発環境である「Xcode」は、自動的に ASLR サポートをオンにして他社製プログラムをコンパイルします。

iOS では、メモリページを実行不可能としてマークする ARM の Execute Never（XN）機能を使用することで保護をさらに強化しています。書き込み可能と実行可能の両方としてマークされたメモリページは、厳しく条件が管理された App のみが使用できます。カーネルによって Apple 独自の動的コード署名エンタイトルメントの有無が確認されます。この場合でも、ランダムなアドレスが与えられた実行可能かつ書き込み可能なページを要求するために、1 回の mmap 呼び出ししか発行できません。「Safari」では、JavaScript JIT コンパイラでこの機能が使用されます。

機能拡張

iOS では、機能拡張を提供することで、App の機能をほかの App に提供できます。 機能拡張は、署名された特殊な目的を持つ実行可能バイナリで、 App 内にパッケージ化されています。 App のインストール時に機能拡張が自動的に検出され、 対応するシステムを持ったほかの App で利用できるようになります。

機能拡張をサポートするシステム領域は、 拡張ポイントと呼ばれます。 それぞれの拡張ポイントが API を提供し、その領域のポリシーを適用します。 システムは、拡張ポイント固有のマッチングルールに基づいて、 利用できる機能拡張を判断します。 システムは必要に応じて機能拡張プロセスを自動的に起動し、 そのプロセスの終了まで管理します。 また、 エンタイトルメントを使うと、 機能拡張の利用可否を特定のシステム App に制限できます。 たとえば、「今日」 表示ウィジェットは通知センターにだけ表示され、 共有機能拡張は「共有」 パネルからのみ利用できます。 拡張ポイントには、「今日」 ウィジェット、 共有、 カスタムアクション、 写真編集、ドキュメントプロバイダ、 カスタムキーボードがあります。

機能拡張は、 自身のアドレス空間内で実行されます。 機能拡張と機能拡張を起動した App 間の通信には、 システムフレームワークが仲介するプロセス間通信が使用されます。 互いのファイルやメモリ空間にはアクセスできません。 機能拡張は、 機能拡張同士、 機能拡張を含む App 本体、および機能拡張を使用する App からは互いに隔離されるように設計されています。 ほかの他社製 App と同様にサンドボックス化され、 機能拡張を含む App 本体のコンテナとは別のコンテナを持ちます。 ただし、 プライバシーコントロールへのアクセスは、 App 本体と同じものになります。そのため、 ユーザが App に「連絡先」 へのアクセス権を付与した場合、 このアクセス権はその App に埋め込まれた機能拡張に対しては適用されますが、 その App が起動する別の App の機能拡張には適用されません。

カスタムキーボードは、ユーザが有効にするとシステム全体に適用される特殊な種類の機能拡張です。有効にすると、 パスコードの入力とテキストのセキュア表示以外のすべてのテキストフィールドでキーボード機能拡張が使用されます。 ユーザデータの転送を制限するため、 カスタムキーボードはデフォルトで厳しく制限されたサンドボックス内で実行されます。 これにより、 ネットワーク、 プロセスに代わってネットワーク操作を実行するサービス、 および入力データの漏洩が可能な API へのアクセスがブロックされます。 カスタムキーボードのデベロッパは、 機能拡張に Open Access を付与することを要求できます。 これにより、 その機能拡張は、 ユーザの同意を得た後にデフォルトのサンドボックス内で実行できるようになります。

MDM ソリューションに登録されたデバイスでは、 書類とキーボードの機能拡張は Managed Open In ルールに従って動作します。 たとえば、 MDM ソリューションは、 ユーザが管理対象 App から管理対象外ドキュメントプロバイダに書類を書き出したり、 管理対象 App 内で管理対象外キーボードを使用したりすることを禁止できます。 また、 App のデベロッパは App 内で他社製のキーボード機能拡張の使用を禁止することもできます。

App グループ

特定のデベロッパアカウントが所有する App と機能拡張では、 App グループの一部として構成することで、 コンテンツを共有できるようになります。 デベロッパは任意で Apple Developer Portal 上で適切なグループを作成し、 目的の App と機能拡張をそのグループに追加できます。App グループのメンバーとして構成されると、 App には以下の項目へのアクセス権が付与されます。

- データ保存用の共有オンボリュームコンテナ （そのグループの App が 1 つ以上インストールされている限りデバイス上に残ります）
- 共有される環境設定
- 共有されるキーチェーン項目

Apple Developer Portal により、 App のエコシステム全体での App グループ ID の一意性が保証されます。

App 内のデータ保護

iOS の Software Development Kit（SDK）は完全な API 一式を提供しており、社内外のデベロッパはデータ保護を採用し、最高レベルの保護を App 内で達成できるようにする API がすべて揃っています。データ保護は、NSFileManager、CoreData、NSData、および SQLite などのファイル API とデータベース API で利用できます。

「メール」App のデータベース（添付ファイルを含む）、管理対象のブック、Safari ブックマーク、App の起動イメージ、および位置情報データについても、ユーザのパスコードによって保護された鍵で暗号化されてデバイスに保存されます。カレンダー（添付ファイルを除く）、連絡先、リマインダー、メモ、メッセージ、および写真には、Protected Until First User Authentication のデータ保護エンタイトルメントが適用されます。

ユーザがインストールした App のうち、特定のデータ保護クラスに所属していない App には、デフォルトで Protected Until First User Authentication が割り当てられます。

アクセサリ

Made for iPhone/iPad/iPod touch（MFi）ライセンスプログラムでは、審査を通過したアクセサリメーカーは iPod Accessories Protocol（iAP）および必要な対応ハードウェアコンポーネントにアクセスできます。

MFi アクセサリが Lightning コネクタまたは Bluetooth 経由で iOS と通信するときは、デバイスがアクセサリに対して、Apple による認定を受けた証明として Apple 発行の証明書での応答を求め、その証明書を検証します。その後デバイスがチャレンジを送信し、アクセサリはそれに対して署名付きの応答で答える必要があります。このプロセスはすべて Apple が認定アクセサリメーカーに提供するカスタム集積回路（IC）で処理されるため、アクセサリ自体に対しては透過的なプロセスです。

アクセサリは、別の伝送方法や伝送機能へのアクセス（Lightning ケーブル経由でのデジタル・オーディオ・ストリームへのアクセスや、Bluetooth 経由での位置情報の提供など）を要求できます。認証 IC によって、認定アクセサリにのみデバイスへのフルアクセスが付与されます。アクセサリが認証処理に対応していない場合、アクセスはアナログオーディオおよび一部のシリアル（UART）オーディオ再生コントロールに限定されます。

AirPlay でも、認証 IC を使用して、レシーバが Apple によって認定されていることを確認します。AirPlay オーディオおよび CarPlay ビデオストリームでは、MFi-SAP（Secure Association Protocol）を利用して、アクセサリとデバイス間の通信が AES-128 の CTR モードで暗号化されます。また、Station-to-Station（STS）プロトコルの一部として、一時鍵が ECDH 鍵交換（Curve25519）により交換され、認証 IC の 1024 ビット RSA 鍵を使って署名されます。

HomeKit

HomeKit は、ホームオートメーションのインフラストラクチャで、iCloud と iOS のセキュリティ機能を利用して個人データを保護しながら同期できます。個人データは Apple に開示されません。

HomeKit 識別情報

HomeKit の識別情報とセキュリティは、Ed25519 公開／秘密鍵ペアに基づいています。Ed25519 鍵ペアは、HomeKit のユーザごとに iOS デバイス上で生成され、それがそのユーザの HomeKit 識別情報となります。この鍵ペアを使用して、iOS デバイス間および iOS デバイスとアクセサリ間の通信が認証されます。

これらの鍵はキーチェーンに保存され、暗号化されたキーチェーンのバックアップにのみ含められます。また、iCloud キーチェーンが利用可能な場合は、それを通じてデバイス間で同期されます。HomePod と Apple TV は、タップして設定プロセスまたは設定モードで鍵を受け取ります（下記参照）。Apple Watch には、ペアリングされた iPhone から Apple Identity Service（IDS）を介して鍵が共有されます。

HomeKit 対応アクセサリとの通信

HomeKit 対応アクセサリは、iOS デバイスとの通信に使用する固有の Ed25519 鍵ペアを生成します。アクセサリが工場出荷時の設定に復元されると、新しい鍵ペアが生成されます。

iOS デバイスと HomeKit 対応アクセサリ間の接続を確立するため、アクセサリメーカーから提供された 8 桁のコードをユーザが iOS デバイスに入力して、Secure Remote Password（3072 ビット）プロトコルによる鍵の交換を行うと、HKDF-SHA-512 から導出された鍵を用いた CHACHA20-POLY1305 AEAD によって鍵が暗号化されます。アクセサリの MFi 証明書も設定中に検証されます。MFi チップを搭載していないアクセサリの場合、iOS 11.3 以降ではソフトウェア認証のサポートを組み込むことができます。

使用時に iOS デバイスと HomeKit 対応アクセサリが通信する場合は、上記のプロセスで交換された鍵を使用して互いに認証します。各セッションは Station-to-Station プロトコルを使用して確立され、セッションごとの Curve25519 鍵に基づく、HKDF-SHA-512 から導出された鍵で暗号化されます。これは、IP ベースと Bluetooth Low Energy 両方のアクセサリに適用されます。

ブロードキャスト通知をサポートする Bluetooth Low Energy デバイスの場合、ペアリングされた iOS デバイスが、安全なセッションでブロードキャスト暗号鍵を用いてアクセサリをプロビジョニングします。この鍵は Bluetooth Low Energy アドバタイズによって通知される、アクセサリの状態変更に関するデータの暗号化にも使用されます。ブロードキャスト暗号鍵は HKDF-SHA-512 から導出された鍵であり、データは CHACHA20-POLY1305 認証付き暗号（AEAD）アルゴリズムで暗号化されます。このブロードキャスト暗号鍵は iOS デバイスによって定期的に変更され、iCloud 経由でほかのデバイスと同期されます（下記「デバイス間とユーザ間のデータ同期」セクションを参照）。

ローカル・データ・ストレージ

HomeKit はユーザの iOS デバイスに、ホーム、アクセサリ、シーン、およびユーザに関するデータを保存します。保存されるデータは、ユーザの HomeKit 識別情報鍵から導出された鍵と、ランダムなノンスを使用して暗号化されます。さらに、HomeKit データは、Protected Until First User Authentication のデータ保護クラスを使用して保存されます。HomeKit データは暗号化されたバックアップにのみバックアップされます。たとえば、暗号化されていない iTunes バックアップに HomeKit データは含まれません。

デバイス間とユーザ間のデータ同期

HomeKit データは、iCloud と iCloud キーチェーンを使って、1 人のユーザの iOS デバイス間で同期できます。HomeKit データは、ユーザの HomeKit 識別情報から導出された鍵とランダムなノンスを使用して、同期中に暗号化されます。このデータは、同期中は不透明な BLOB として処理されます。最新の BLOB が iCloud に保存されて同期に使用されますが、それは他のいかなる目的にも用いられません。HomeKit データはユーザの iOS デバイスでのみ利用できる鍵を使って暗号化されるため、転送中や iCloud での保管中にその内容を読み取ることはできません。

HomeKit データは、同じホームの複数のユーザ間でも同期されます。このプロセスでは、iOS デバイスと HomeKit アクセサリ間で使用される認証と暗号化と同じものが使用されます。この認証は、ユーザがホームに追加されたときにデバイス間で交換される Ed25519 公開鍵を用いて行われます。新しいユーザがホームに追加されると、それ以降のすべての通信が、Station-to-Station プロトコルとセッションごとの鍵を使用して認証および暗号化されます。

新しいユーザを追加できるのは、HomeKit でそのホームを最初に作成したユーザか、編集権限のある別のユーザです。所有者のデバイスは、アクセサリが新しいユーザを認証し、新しいユーザからのコマンドを受け付けることができるように、新しいユーザの公開鍵を使ってアクセサリを構成します。編集権限のあるユーザが新しいユーザを追加した場合、このプロセスはホームハブに委任されて処理が完了します。

ユーザが iCloud にサインインすると、 Apple TV を HomeKit で使用するためのプロビジョニングプロセスが自動的に実行されます。 iCloud アカウントでは 2 ファクタ認証を有効にしておく必要があります。 Apple TV と所有者のデバイスは、 一時的な Ed25519 公開鍵を iCloud 経由で交換します。 所有者のデバイスと Apple TV が同じローカルネットワーク上にあるときにこの一時鍵が使用され、 ローカルネットワーク上の接続が Station-to-Station プロトコルとセッションごとの鍵によってセキュリティ保護されます。 このプロセスでは、 iOS デバイスと HomeKit アクセサリ間で使用される認証と暗号化と同じものが使用されます。 このセキュリティ保護されたローカル接続を経由して、 所有者のデバイスは Apple TV にユーザの Ed25519 公開／秘密鍵ペアを転送します。 その後はこれらの鍵を使用して Apple TV と HomeKit 対応アクセサリ間の通信、 および Apple TV と HomeKit ホームの一部であるその他の iOS デバイス間の通信をセキュリティ保護します。

複数のデバイスを使用していないユーザが、 追加ユーザによるホームへのアクセスを許可しない場合、 HomeKit データは iCloud に同期されません。

ホームデータと App

App によるホームデータへのアクセスは、 ユーザの「プライバシー」 設定で制御されます。 App がホームデータへのアクセスを要求すると、「連絡先」 や「写真」 などの iOS データソースの場合と同様に、 ユーザにアクセスの許可が求められます。 ユーザが承認すると、 部屋やアクセサリの名前、 各アクセサリが設置されている部屋などの情報に App からアクセスできるようになります。 詳しくは、 developer.apple.com/homekit （英語） にある HomeKit デベロッパ向けマニュアルを参照してください。

HomeKit と Siri

Siri を使って、 アクセサリに対するクエリや制御、 シーンの起動を行うことができます。 Siri がコマンドを認識できるように、 部屋、 アクセサリ、 シーンの名前を提供する必要がありますが、 Siri に提供されるのはホームの構成に関する最低限の情報で、 個人も特定されません。 Siri に送られた音声は特定のアクセサリまたはコマンドを示す場合がありますが、 このようなデータが HomeKit などの Apple のその他の機能に関連付けられることはありません。 詳しくは、 この文書の「インターネットサービス」 セクションにある「Siri」 を参照してください。

HomeKit 対応 IP カメラ

HomeKit 対応の IP カメラはビデオストリームおよびオーディオストリームを、 ローカルネットワーク上にあり、 それらのストリームにアクセスしている iOS デバイスに直接送信します。 ストリームは iOS デバイスおよび IP カメラでランダムに生成される鍵を使って暗号化され、 これらの鍵はカメラとの安全な HomeKit セッションを介して交換されます。 iOS デバイスがローカルネットワーク上にない場合は、 暗号化されたストリームがホームハブ経由で iOS デバイスに中継されます。 ホームハブはストリームを復号せず、 iOS デバイスと IP カメラ間の中継としてのみ機能します。 HomeKit 対応の IP カメラが撮影したビデオ映像を App でユーザに表示するときは、 HomeKit が別のシステムプロセスを使ってビデオフレームを安全に処理します。 App が直接ビデオストリームにアクセスしたり保存したりすることはできません。 また、 このストリームからのスクリーンショットを App から取得することも許可されません。

HomeKit 対応アクセサリへの iCloud リモートアクセス

HomeKit 対応アクセサリは、 Bluetooth や Wi-Fi が使用できない場合に iOS デバイスがアクセサリを制御できるように、 iCloud に直接接続することができます。

iCloud リモートアクセスはセキュリティを十分に配慮して設計されており、 アクセサリを制御したりアクセサリから通知を送信したりするときに、 アクセサリ自体の情報や送信中のコマンドおよび通知の内容が Apple に公開されることはありません。 HomeKit は、 ホームに関する情報を iCloud リモートアクセス経由で送信しません。

ユーザが iCloud リモートアクセスを使ってコマンドを送信するときは、 アクセサリと iOS デバイスが相互に認証し、 ローカル接続で説明した手順と同じ方法でデータが暗号化されます。 通信内容は暗号化されるため、 Apple がその内容を見ることはできません。 iCloud 経由でのアドレス指定は、 設定プロセス中に登録された iCloud 識別子に基づいて行われます。

iCloud リモートアクセスをサポートしているアクセサリは、アクセサリの設定プロセス時にプロビジョニングされます。プロビジョニングプロセスは、ユーザが iCloud にサインインすると開始されます。次に、iOS デバイスは、すべての Built for HomeKit アクセサリに内蔵されている Apple 認証コプロセッサを使ってチャレンジに署名するようにアクセサリに要求します。アクセサリは prime256v1 楕円曲線鍵も生成し、署名されたチャレンジおよび認証コプロセッサの X.509 証明書と共に公開鍵が iOS デバイスに送信されます。これらは、iCloud プロビジョニングサーバからアクセサリの証明書を要求するために使用されます。証明書はアクセサリに保存されますが、HomeKit iCloud リモートアクセスへのアクセス権が付与されているという情報を除き、アクセサリを特定する情報は含まれません。また、プロビジョニングを実行中の iOS デバイスはアクセサリにバッグも送信します。このバッグには、iCloud リモートアクセス・サーバへの接続に必要な URL などの情報が含まれています。この情報はユーザやアクセサリに特有のものではありません。

各アクセサリは、許可したユーザのリストを iCloud リモートアクセス・サーバに登録します。これらのユーザは、アクセサリをホームに追加した人によってアクセサリの制御権限が付与されたユーザです。ユーザには iCloud サーバによって識別子が付与されます。また、アクセサリからの通知メッセージおよび応答を配信する目的で iCloud アカウントにユーザを割り当てることもできます。同様に、アクセサリには iCloud から発行された識別子が付与されますが、これらの識別子は不明瞭な情報となっているため、アクセサリ自体のことについては何も分かりません。

アクセサリは HomeKit iCloud リモートアクセス・サーバに接続するときに証明書とパスを提示します。このパスは別の iCloud サーバから取得されたもので、各アクセサリに固有のものではありません。アクセサリがパスを要求するとき、その要求にはアクセサリのメーカー、モデル、およびファームウェアバージョンが含まれます。この要求では、ユーザまたはホームを特定できる情報は送信されません。プライバシーを保護するため、パスサーバへの接続は認証されません。

アクセサリが iCloud リモートアクセス・サーバに接続するときは、HTTP/2 が使用され、TLS v1.2（AES-128-GCM と SHA-256 を使用）によってセキュリティが確保されます。アクセサリから iCloud リモートアクセス・サーバへの接続は開いたまま維持されるので、アクセサリは着信メッセージを受信したり、応答や通知を iOS デバイスに送信したりできます。

HomeKit 対応テレビ・リモコン・アクセサリ

他社製の HomeKit 対応テレビ・リモコン・アクセサリは、「ホーム」App で追加され関連付けられた Apple TV に HID イベントと Siri オーディオを提供します。HID イベントは、Apple TV とリモコン間で確立された安全なセッションを介して送信されます。Siri 対応のテレビリモコンでは、ユーザが専用の Siri ボタンを使用してリモコンのマイクを明示的に有効にしたときに、Apple TV にオーディオデータが送信されます。オーディオフレームは、Apple TV とリモコン間の専用ローカルネットワーク接続を通じて Apple TV に直接送信されます。このローカルネットワーク接続は、HKDF-SHA-512 から導出されるセッションごとの鍵ペアで暗号化されます。また、この鍵ペアは、Apple TV とテレビリモコン間で確立された HomeKit セッションでネゴシエートされます。オーディオフレームは Apple TV 上で復号されてから「Siri」App に転送され、そこでほかの Siri オーディオ入力と同じプライバシー保護レベルで扱われます。

SiriKit

Siri は iOS の機能拡張メカニズムを利用して他社製 App と通信します。Siri は iOS の連絡先やデバイスの現在地にアクセスできますが、機能拡張を含む App にそれらの情報を提供するときは、まず App のアクセス権を調べて、iOS で保護されているユーザデータへのアクセスが許可されているかどうかを確認します。Siri は、ユーザによる元のクエリテキストからの関連部分のみを機能拡張に渡します。たとえば、App には iOS 連絡先へのアクセス権がない場合、Siri は「支払い App を使ってお母さんに 10 ドル支払って」というユーザリクエスト内の関連性を解決しません。つまりこの場合、機能拡張の App は、「お母さん」という言葉を App に渡される生の音声としてのみ認識します。一方、App に iOS 連絡先へのアクセス権がある場合、App はユーザの母親に関する iOS 連絡先情報を受け取ります。また、「兄さんはすごい、と「メッセージ」

App でお母さんに伝えて」など、連絡先がメッセージ本文で言及されている場合、Siri は App の TCC に関係なく「兄さん」という言葉の関係性を解決しません。App によって提示されるコンテンツは、ユーザが App で使用する言葉を Siri が認識できるようにするため、サーバに送信される場合があります。「<App 名 > でお母さんの家まで配車を手配して」のように、ユーザのリクエストでユーザの連絡先から位置情報を取得する必要がある場合は、App が持つ位置情報および連絡先へのアクセス権にかかわらず、そのリクエストにおいてのみ、Siri から App の機能拡張に位置情報が提供されます。

Siri は実行時に SiriKit 対応 App がアプリケーションインスタンスに固有のカスタムの単語一式を提供することを許可します。カスタムの単語は、この文書の「Siri」セクションで説明されているランダムな識別子に関連付けられ、その識別子と同じライフタイムを持ちます。

HealthKit

HealthKit は、ユーザの許可を得てヘルスケアおよびフィットネス App のデータを保存および集計します。HealthKit は、互換性のある Bluetooth Low Energy（BLE）心拍モニタのようなヘルスケアやフィットネス関連のデバイスや、多くの iOS デバイスに内蔵されているモーションコプロセッサとも直接連係します。

ヘルスケアデータ

HealthKit では、App、デバイス、医療機関といったソースから収集されたヘルスケアデータを、ユーザが保存および集計できます。このデータは、データ保護クラス Protected Unless Open で保存されます。このデータは、デバイスがロックされてから 10 分後にアクセスできなくなり、ユーザが次回パスコードを入力するか、Touch ID または Face ID を使用してロック解除したときにアクセス可能になります。

HealthKit では、App 用のアクセス権、HealthKit に接続されているデバイス、新しいデータが利用可能になったときに App を起動するスケジュール情報などの管理データも 1 か所で管理できます。これらのデータは、データ保護クラス Protected Until First User Authentication で保存されます。

ユーザが運動しているときなど、デバイスがロックされている間に生成されるヘルスケアレコードは、一時的なジャーナルファイルに保存されます。これらのデータは、データ保護クラス Protected Unless Open で保存されます。デバイスがロック解除されると、この一時的なジャーナルファイルが主要なヘルスケアデータベースに読み込まれ、マージされた後に削除されます。

ヘルスケアデータは iCloud に保存できます。ヘルスケアデータを iCloud に保存するように構成すると、データはデバイス間で同期され、送信中も保存時もデータは暗号化されるので、セキュリティも確保されます。ヘルスケアデータは、暗号化された iTunes バックアップにのみ保存されます。暗号化されていない iTunes バックアップや iCloud バックアップには保存されません。

診療記録

ユーザは、「ヘルスケア」App 内から対応するヘルスケアシステムにログインして、診療記録のコピーを取得できます。ヘルスケアシステムに接続するときは、OAuth 2 クライアント資格情報を使用してユーザ認証が行われます。接続後は、TLS v1.2 で保護された接続を介して診療記録データが医療機関から直接ダウンロードされます。ダウンロードした診療記録は、ほかのヘルスケアデータと共に安全に保管されます。

データの完全性

データベースに保存されるデータには、各データレコードの出自を追跡するためのメタデータが含まれます。このメタデータには、当該レコードを保存した App を特定する App 識別子が含まれます。さらに、オプションのメタデータ項目には、当該レコードのデジタル署名されたコピーを含めることができます。これは、信頼できるデバイスによって生成されたレコードにデータの完全性を付与するためです。デジタル署名には、IETF RFC 5652 で定められている CMS（Cryptographic Message Syntax）が使用されます。

他社製 App によるアクセス

HealthKit API へのアクセスはエンタイトルメントで制御され、 App は、 データの利用方法に関する制限に従う必要があります。 たとえば、 ヘルスケアデータを広告に利用することはできません。 また、 ヘルスケアデータの利用について詳細に規定したプライバシーポリシーをユーザに提示することも要求されます。

App によるヘルスケアデータへのアクセスは、 ユーザの「プライバシー」 設定で制御されます。 App がヘルスケアデータへのアクセスを要求すると、「連絡先」や「写真」などの iOS データソースの場合と同様に、ユーザにアクセスの許可が求められます。 ただし、ヘルスケアデータの場合は、データの種類ごとに別々のアクセス許可が必要となるほか、 データの読み取りと書き込みにも別々のアクセス許可が必要です。 ユーザは、「ヘルスケア」 App の「ソース」 タブで、ヘルスケアデータのアクセスに関して付与した権限を確認および取り消すことができます。

App にデータの書き込み権限が付与されている場合は、 書き込んだデータを読み取ることもできます。 データの読み取り権限が付与されている場合は、 すべてのソースによって書き込まれたデータを読み取ることができます。 ただし、 App から、 ほかの App に付与されたアクセス権を調べることはできません。 また、 App 側でその App にヘルスケアデータの読み取り権限が付与されたかどうかを確定的に知る方法もありません。 App に読み取り権限がない場合は、 どのクエリでも空のデータが返されます。 これは、空のデータベースからの応答と同じ動作なので、App はユーザの追跡しているデータの種類を把握して、 ユーザの健康状態を推測することができなくなります。

メディカル ID

「ヘルスケア」 App では、 医療上の緊急事態に備えて、 重要な情報をメディカル ID フォームに入力しておくことができます。 この情報は手動で入力や、 更新を行います。 また、 ヘルスケアデータベースの情報とは同期されません。

メディカル ID 情報は、 ロック画面の緊急ボタンをタップすると表示されます。 この情報はデータ保護クラス **No Protection** を使用してデバイスに保存されているため、 デバイスのパスコードを入力しなくてもアクセスできます。 メディカル ID は、 安全とプライバシーに関する懸念のバランスをどのように取るかをユーザが自分で決定できるオプション機能です。 このデータは iCloud バックアップにバックアップされますが、 CloudKit を介してデバイス間で同期されることはありません。

ReplayKit

ReplayKit はデベロッパが録画やライブブロードキャスト機能を App に追加することを実現するフレームワークです。 また、ユーザはデバイスの前面のカメラとマイクを使用して、録画やブロードキャストに注釈を加えることもできます。

ムービーの収録

ムービーの収録機能には、 何層ものセキュリティ機能が埋め込まれています。

- **許可を求めるダイアログ：** 収録開始前に、 ReplayKit は、 ユーザが画面、 マイク、 および前面カメラを収録する意図があることを確認する注意画面を表示し、 同意を求めます。 この画面は、 App プロセスごとに 1 回表示され、 App がバックグラウンドにある状態が 8 分を超えた場合も表示されます。
- **画面および音声の取り込み：** 画面および音声の取り込みは App のプロセス内ではなく、 ReplayKit デーモン **replayd** 内で実行されます。 これにより、 収録されたコンテンツが App プロセスからはアクセスできないことが保証されます。
- **ムービーの作成および保存：** ムービーファイルは ReplayKit のサブシステムのみがアクセスできるディレクトリに書き込まれるので、App からはアクセスできません。 これにより、収録がユーザの同意なく第三者によって使用されることを防止します。
- **エンドユーザによるプレビューおよび共有：** ユーザは ReplayKit によって提供される UI を使用してムービーをプレビューおよび共有できます。この UI は、iOS 機能拡張インフラストラクチャにより別のプロセスを使って表示され、 生成されたムービーファイルにアクセスします。

ブロードキャスト

- **画面および音声の取り込み：**ブロードキャスト中の画面および音声取り込みは、ムービーの収録と同様に replayd 内で実行されます。
- **ブロードキャスト機能拡張：**他社製サービスが ReplayKit ブロードキャストに加わる場合、com.apple.broadcast-services エンドポイントで構成される新しい機能拡張を 2 つ作成する必要があります。
  - ユーザがブロードキャストを設定できる UI 機能拡張
  - ビデオおよび音声データをサービスのバックエンドサーバにアップロードするアップロード機能拡張

アーキテクチャによって、ホスト側の App が、ブロードキャストされるビデオおよび音声コンテンツへのアクセス権を持たないことが保証されます。ReplayKit および他社製ブロードキャスト機能拡張のみがアクセス権を持ちます。

- **ブロードキャストピッカー：**ReplayKit には、使用するブロードキャストサービスを選択するために、デベロッパが App 内で表示できる View Controller（UIActivityViewController と同様）が用意されています。この View Controller は、UIRemoteViewController SPI を使用して実装され、ReplayKit フレームワーク内で動作する機能拡張です。これはホスト側 App とは別のプロセス空間で実行されます。
- **システム・ブロードキャスト・ピッカー：**コントロールセンターからアクセスできるシステム定義の UI を使用して、ユーザが App 内から直接、システムブロードキャストを開始できます。この UI は UIRemoteViewController SPI を使用して実装され、ReplayKit フレームワーク内で動作する機能拡張です。これはホスト側 App とは別のプロセス空間で実行されます。
- **アップロード機能拡張：**ブロードキャスト中のビデオおよび音声コンテンツを処理するために他社製ブロードキャストサービスが実装するアップロード機能拡張では、2 つのコンテンツ受信方法を選択できます。
  - エンコードされた小さな MP4 クリップ
  - エンコードされていない生のサンプルバッファ

    - **MP4 クリップの処理：**この処理モードでは、エンコードされた小さな MP4 クリップが replayd によって生成され、ReplayKit のサブシステムのみがアクセス可能なプライバシーが保護された場所に保存されます。ムービークリップが生成されると、replayd は NSExtension リクエスト SPI（XPC ベース）を通じて他社製アップロード機能拡張にムービークリップの場所を渡します。replayd は、ワンタイム・サンドボックス・トークンも生成し、これもアップロード機能拡張に渡されます。このトークンにより、機能拡張がリクエスト中に特定のムービークリップへアクセスすることが許可されます。
    - **サンプルバッファの処理：**この処理モードでは、ビデオおよび音声データはシリアライズされ、直接 XPC 接続を通じて他社製アップロード機能拡張にリアルタイムで渡されます。ビデオデータは、ビデオ・サンプル・バッファから IOSurface オブジェクトを抽出することでエンコードされ、XPC オブジェクトとして安全にエンコードされます。このデータは、XPC 経由で他社製の機能拡張に送信され、そこで IOSurface オブジェクトへ安全にデコードされます。

秘密メモ

「メモ」App には、秘密メモの機能が搭載されており、ユーザは特定のメモの内容を保護できます。秘密メモはユーザが設定したパスフレーズで暗号化され、このメモを iOS、macOS、iCloud の Web サイトで表示するには、このパスフレーズが必要になります。

ユーザがメモを保護して秘密メモを作成すると、ユーザのパスフレーズから、PBKDF2 および SHA256 を使って 16 バイトの鍵が導出されます。メモの内容は AES-GCM で暗号化されます。新しいレコードが Core Data および CloudKit 内に作成され、暗号化されたメモ、タグ、および初期化ベクトルが保存されます。元のメモのレコードは削除され、そこに暗号化されたデータが書き込まれることはありません。添付ファイルも同じように暗号化されます。秘密メモでは、

イメージ、スケッチ、表、マップ、および Web サイトの添付ファイルがサポートされます。ほかの種類の添付ファイルを含むメモは暗号化できず、サポートされていない添付ファイルを秘密メモに追加することもできません。

秘密メモを表示または作成するときに、ユーザがパスフレーズを正しく入力すると、「メモ」は安全なセッションを開始します。セッション中は、ほかのメモを表示したり秘密メモに設定したりする際に、パスフレーズの入力や Touch ID または Face ID の使用を求められることはありません。ただし、異なるパスフレーズが設定されているメモがある場合、安全なセッションは現在のパスフレーズで保護されているメモにのみ適用されます。安全なセッションは以下の場合に終了します。

- ユーザが「メモ」で「今すぐロック」ボタンをタップした。
- 「メモ」がバックグラウンドに切り替えられてから 3 分を超えた。
- デバイスがロックされた。

ユーザがパスフレーズを忘れても、Touch ID または Face ID がデバイスで有効になっていれば、秘密メモを表示したりほかのメモを秘密メモに設定したりできます。また、パスフレーズの入力に 3 回失敗すると、ユーザが設定したヒントが表示されます。パスフレーズを変更するには、現在のパスフレーズを知っている必要があります。

現在のパスフレーズを忘れた場合は、そのパスフレーズをリセットできます。リセットした場合、新しいパスフレーズで新しい秘密メモを作成することはできますが、以前の秘密メモを表示することはできません。リセット後でも、古いパスフレーズを思い出すことができれば、以前の秘密メモを表示できます。パスフレーズをリセットするには、ユーザの iCloud アカウントのパスフレーズが必要です。

共有メモ

メモはほかのユーザと共有できます。共有メモはエンドツーエンドで暗号化されませんが、ユーザがメモに入力したテキストまたは添付ファイルに、CloudKit で暗号化されるデータ・タイプが使用されます。アセットは CKRecord に含まれる暗号化された鍵により、常に暗号化されています。作成日や変更日などのメタデータは暗号化されません。CloudKit は参加者が互いのデータを暗号化および復号するプロセスを管理します。

Apple Watch

Apple Watch は、iOS 用に構築されたセキュリティ機能とセキュリティ技術を使用して、デバイス上のデータを保護したり、ペアリングされた iPhone やインターネットと通信したりします。これには、データ保護やキーチェーンアクセス制御などの技術が含まれます。ユーザのパスコードも、暗号鍵を作成するためにデバイス UID と関連付けられます。

Apple Watch と iPhone のペアリングは、OOB（帯域外）プロセスで公開鍵を交換し、その後、Bluetooth Low Energy（BLE）リンクの共有シークレットを使用して保護されます。Apple Watch には、iPhone のカメラで読み取るためのアニメーションパターンが表示されます。このパターンには、BLE 4.1 のアウトオブバンドのペアリングに使用されるエンコードされたシークレットが含まれています。必要に応じて、代替ペアリング方式として標準の BLE パスキー入力を使用できます。

Bluetooth Low Energy セッションが確立され、Bluetooth コア仕様で使用可能な最高レベルのセキュリティプロトコルを使用して暗号化されると、Apple Watch と iPhone 間で、Apple Identity Service（IDS）のプロセスを使用して鍵が交換されます（この文書の「インターネットサービス」にある「iMessage」を参照）。鍵が交換されると、Bluetooth セッション鍵が破棄され、Apple Watch と iPhone 間のすべての通信が IDS を使用して暗号化されます。また、暗号化された Bluetooth、Wi-Fi、モバイルデータ通信のリンクも二次的な暗号化レイヤーを提供します。トラフィックが危殆化するリスクを減らすため、Low Energy Bluetooth アドレスは 15 分間隔でローテーションされます。

データのストリーミングが必要な App をサポートするため、この文書の「インターネットサービス」セクションにある「FaceTime」に説明されている方式で暗号化が提供されます。 この方式では、ペアリングされた iPhone が提供する IDS サービス、または直接のインターネット接続が使用されます。

Apple Watch には、この文書の「暗号化とデータ保護」セクションに説明されているように、ハードウェアで暗号化されたストレージとファイル／キーチェーン項目のクラスベースの保護が実装されています。 また、キーチェーン項目用のアクセス制御されたキーバッグも使用されます。 Apple Watch と iPhone 間の通信に使用される鍵も、クラスベースの保護を使用して保護されます。

Apple Watch が Bluetooth の通信範囲内にない場合は、代わりに Wi-Fi またはモバイルデータ通信を使用できます。 Apple Watch は、ペアリングされた iPhone ですでに接続され、両デバイスが通信範囲内にあるときにその資格情報が Apple Watch に同期されている Wi-Fi ネットワークに、自動的に参加します。 この自動接続の動作は、接続後、Apple Watch の「設定」App の「Wi-Fi」セクションでネットワークごとに設定できます。 いずれのデバイスでも以前に接続したことのない Wi-Fi ネットワークの場合は、Apple Watch の「設定」App の「Wi-Fi」セクションから手動で接続できます。

Apple Watch と iPhone が互いの通信範囲内にないときは、ペアリングされた iPhone とインターネット経由でメールデータを同期する代わりに、Apple Watch が iCloud サーバや Gmail サーバに直接接続してメールを取得します。 Gmail アカウントを使用する場合、ユーザは、iPhone の「Watch」App の「メール」セクションで Google への認証を求められます。 Google から受け取った OAuth トークンが Apple Identity Service（IDS）経由で暗号化されて Apple Watch に送信され、メールの取得に使用されます。 この OAuth トークンは、ペアリングされた iPhone から Gmail サーバに接続するときには使用されません。

Apple Watch を手動でロックするには、サイドボタンを押したままにします。 また、手首検出がオンの場合は、Apple Watch を手首から外すとすぐに、自動的にロックされます。 Apple Watch がロックされていると、Apple Pay は Apple Watch のパスコードを入力した場合にのみ使用できます。 手首検出をオフにするには、iPhone の「Watch」App を使用します。 また、MDM ソリューションを使用してこの設定を強制的に適用することもできます。

Apple Watch を装着している場合は、ペアリングされた iPhone を使用して Apple Watch のロックを解除することもできます。 これは、ペアリング中に確立された鍵を使用して認証される接続によって行われます。 iPhone がこの鍵を送信すると、Apple Watch がこの鍵を使用してデータ保護鍵のロックを解除します。 Apple Watch のパスコードは iPhone 側では把握しておらず、転送されることもありません。 この機能をオフにするには、iPhone の「Watch」App を使用します。

Apple Watch がペアリングできる iPhone は一度に 1 台のみです。 ペアリングを解除すると、iPhone の指示により、Apple Watch からすべてのコンテンツとデータが消去されます。

Apple Watch では、システム・ソフトウェア・アップデートをその日の夜に実行するように設定できます。アップデート時に使用される Apple Watch のパスコードの保存方法について詳しくは、この文書の「キーバッグ」セクションを参照してください。

ペアリングされた iPhone で「iPhone を探す」を有効にすると、Apple Watch 上でもアクティベーションロックの使用が許可されます。 アクティベーションロックにより、Apple Watch の紛失または盗難時に、その Apple Watch を他人が使用または売却することが困難になります。 アクティベーションロックが有効になっている場合、Apple Watch のペアリング解除、消去、再アクティベーションにはそのユーザの Apple ID とパスワードが必要になります。

ネットワークのセキュリティ

iOS デバイスに保存されたデータを保護するために採用された内蔵セキュリティ機能のほかに、ネットワーク上のセキュリティを守るための様々な手段があります。 これにより、 iOS デバイスが送受信する情報の安全性を保つことができます。

モバイルユーザにとって、 世界中どこからでも企業の情報ネットワークにアクセスできることは不可欠です。 その際には、 ユーザの認証と、 データ転送時の保護を確実に行う必要があります。 iOS は、通信の認証、承認、暗号化に標準のネットワークプロトコルを使用し、このプロトコルにデベロッパもアクセスできるようにしています。 iOS では、 このようなセキュリティ上の目標を達成するために、 Wi-Fi 接続とモバイルデータ通信ネットワーク接続の両方で、 実績のあるテクノロジーと、最新の標準規格を統合しています。

ほかのプラットフォームでは、 開いている通信ポートからの侵入を保護するために、 ファイアウォールソフトウェアが必要です。 iOS では、リスニングポートを制限し、 Telnet、 シェル、 Web サーバといった不要なネットワークユーティリティを省くことで、 攻撃領域を狭めているため、 iOS デバイスにファイアウォールソフトウェアを追加する必要はありません。

TLS

iOS は、 Transport Layer Security（TLS v1.0、 TLS v1.1、 TLS v1.2）および DTLS に対応しています。 また、 AES-128 と AES-256 の両方をサポートしており、 PFS（Perfect Forward Secrecy）に対応した暗号スイートを優先的に使用します。 Safari、 カレンダー、 メールなどのインターネットを使う App では、自動的にこのプロトコルを使用して、デバイスとネットワークサービス間の通信チャネルを暗号化します。 ハイレベル API（CFNetwork など）を使うことで、 TLS を App に簡単に導入できるほか、 低レベル API （Network.framework）を使ったきめ細かい制御も可能です。 CFNetwork は SSLv3 の使用を許可せず、 Safari など WebKit を使用する App は SSLv3 接続の確立が禁止されます。

iOS 11 以降および macOS High Sierra 以降では、 SHA-1 証明書はユーザが信頼しない限り TLS 接続に使用できなくなりました。 RSA 鍵が 2048 ビット未満の証明書の使用も禁止されました。 iOS 10 および macOS Sierra では、 RC4 対称暗号スイートが非推奨になっています。 デフォルトでは、 SecureTransport API を使って実装された TLS クライアントまたはサーバで、 RC4 暗号スイートが無効になっているため、 RC4 以外の暗号スイートを利用できない場合は、 接続できません。 セキュリティを強化するため、 RC4 を必要とするサービスまたは App をアップグレードして最新の安全な暗号スイートを使えるようにする必要があります。 iOS 12.1 では、 2018 年 10 月 15 日以降に発行されたシステム信頼済みのルート証明書は、 TLS 接続に使用できるように信頼された Certificate Transparency ログとして公開されている必要があります。

App Transport Security

App Transport Security はデフォルトの接続要件を規定します。 NSURLConnection、 CFURL、 または NSURLSession の各 API の使用時に、 App がベストプラクティスに従って安全に接続できるようになります。 デフォルトでは、 App Transport Security は暗号化方式の選択肢を、 前方秘匿性（Forward Secrecy）を持つ暗号スイートのみに限定しています。 具体的には、 GCM または CBC モードでの ECDHE_ECDSA_AES および ECDHE_RSA_AES のみ使用可能です。 App はドメインごとに前方秘匿性の要件を無効にできます。 この場合、 利用可能な暗号化方式 RSA_AES が追加されます。

サーバは TLS v1.2 と前方秘匿性をサポートしている必要があり、 2048 ビット以上の RSA 鍵または 256 ビット以上の楕円曲線鍵を用いた SHA-256 以上を使って署名された有効な証明書も必要です。

App が App Transport Security が無効にしている場合を除き、 上記の要件を満たさないネットワーク接続は失敗します。 証明書が無効な場合は必ず失敗し、 接続は確立されません。 App Transport Security は iOS 9 以降向けにコンパイルされた App に自動的に適用されます。

VPN

仮想プライベートネットワークなどの安全なネットワークサービスは、 通常、 最小限の設定と構成だけで、 iOS デバイスで使用できるようになります。 iOS デバイスは、 以下のプロトコルと認証方法をサポートする VPN サーバに接続できます。

- IKEv2/IPSec（共有シークレット、 RSA 証明書、 **ECDSA** 証明書、 EAP-MSCHAPv2、 または EAP-TLS による認証）
- SSL-VPN（App Store から入手した適切なクライアント App を使用）
- Cisco IPSec（パスワードによるユーザ認証、および共有シークレットと証明書によるコンピュータ認証）
- L2TP/IPSec（MS-CHAPV2 パスワードによるユーザ認証、 および共有シークレットによるコンピュータ認証）

iOS は以下の VPN 接続に対応しています。

- **VPN オンデマンド**。 証明書ベースの認証を使用するネットワークで使います。 IT ポリシーにより、 VPN 接続が必要なドメインが VPN 構成プロファイルを使って指定されます。
- **Per App VPN**。 VPN 接続を非常に細かく設定することができます。 MDM では、 各管理対象 App や「Safari」の特定のドメインの接続を指定できます。 これにより、セキュアなデータは常に企業ネットワークを経由し、 ユーザの個人データは企業ネットワークを経由しないようにすることができます。
- **VPN 常時接続**。 これは、 モバイルデバイス管理（MDM）ソリューションで管理され、 Apple Configurator 2、 Apple School Manager、 または Apple Business Manager で監視されているデバイスに構成できます。 これにより、 モバイルデータ通信ネットワークおよび Wi-Fi ネットワークに接続するときに、 保護を有効にするためにユーザが VPN をオンにする必要がなくなります。また VPN 常時接続では、組織に向かうすべての IP トラフィックをトンネリングすることで、 組織はデバイスのトラフィックを完全に制御できます。 デフォルトのトンネリングプロトコルである IKEv2 は、 データの暗号化によってトラフィックの転送を保護します。 組織では、デバイスを行き来するトラフィックを監視およびフィルタリングしたり、ネットワーク内のデータをセキュリティ保護したり、 デバイスからインターネットへのアクセスを制限することが可能です。

Wi-Fi

iOS は、 WPA2 Enterprise を含む業界標準の Wi-Fi 規格に対応しており、 企業のワイヤレスネットワークへの認証を用いたアクセスが可能になります。 WPA2 Enterprise は AES-128 暗号化を採用しているため、 ユーザは Wi-Fi ネットワーク接続での送受信時に最高レベルのデータ保護を維持することができます。 また、 802.1X に対応しているので、 さまざまな RADIUS 認証環境に組み込むこともできます。 iPhone および iPad がサポートしている 802.1X ワイヤレス認証方法には、 EAP-TLS、 EAP-TTLS、 EAP-FAST、 EAP-SIM、 PEAPv0、 PEAPv1、 および LEAP があります。

データの保護に加え、 iOS は 802.11w に記載の Protected Management Frame（管理フレーム保護）サービスを通じて、 WPA2 レベルの保護をユニキャストおよびマルチキャスト管理フレームに拡張します。 PMF サポートは、 iPhone 6 以降および iPad Air 2 以降で利用可能です。

iOS は、 Wi-Fi ネットワークに関連付けられていない状態で Wi-Fi スキャンを実行するときに、ランダム化された MAC アドレス（Media Access Control）アドレスを使用します。 このようなスキャンは、 優先する Wi-Fi ネットワークを検索して接続する場合や、 ジオフェンスを使用する App の位置情報サービスを支援するため（位置情報に基づくリマインダーの使用時や「マップ」App での位置情報の修正時など）に実行されることがあります。 優先する Wi-Fi ネットワークへの接続時に実行される Wi-Fi スキャンは、 ランダム化されないので注意が必要です。

デバイスが Wi-Fi ネットワークに関連付けられていないか、 デバイスのプロセッサがスリープ状態にある場合、 iOS は、 enhanced Preferred Network Offload（ePNO）スキャンの実行時にもランダムな MAC アドレスを使用します。 ePNO スキャンは、 位置情報に基づくリマインダーでデバイスが特定の場所の近くにあるかどうかを判定する場合など、 ジオフェンスを使用する App がデバイスの位置情報サービスを利用する際に実行されます。

Wi-Fi ネットワークとの接続が解除されるとデバイスの MAC アドレスが変更されるようになったため、 Wi-Fi トラフィックのパッシブなオブザーバは、 MAC アドレスを使ってデバイスを継続的に追跡できません。 これは、 デバイスがモバイルデータ通信ネットワークに接続されている場合も同様です。 Apple は、 iOS Wi-Fi スキャンがランダムな MAC アドレスを使用すること、 および Apple にもメーカーにもランダムな MAC アドレスの予測は不可能であることを Wi-Fi メーカーにお知らせしてきました。 Wi-Fi MAC アドレスのランダム化は、 iPhone 4s 以前ではサポートされていません。

iPhone 6s 以降では、 既知の Wi-Fi ネットワークの非表示プロパティが自動的に認識され更新されます。 Wi-Fi ネットワークのサービスセット識別子（SSID）がブロードキャストされる場合、 iOS デバイスは、 要求に SSID が含まれるプローブを送信しません。 これにより、 表示されているネットワークのネットワーク名がデバイスによってブロードキャストされることが防止されます。

ネットワークプロセッサのファームウェアの脆弱性からデバイスを保護するため、 Wi-Fi やベースバンドなどのネットワークインターフェイスからアプリケーションプロセッサのメモリへのアクセスは制限されます。 ネットワークプロセッサとのインターフェイスに USB または SDIO が使用されている場合、 ネットワークプロセッサはアプリケーションプロセッサへのダイレクトメモリアクセス（DMA）トランザクションを開始できません。 PCIe が使用されている場合、 各ネットワークプロセッサはそれぞれ専用の隔離された PCIe バス上にあります。 各 PCIe バスの IOMMU により、 ネットワークプロセッサからの DMA アクセスは、 そのネットワークプロセッサのネットワークパケットまたは制御構造を含むメモリページのみに制限されます。

Bluetooth

iOS の Bluetooth サポートは、 個人データへのアクセスを不必要に増やすことなく、 便利な機能を提供できるように設計されています。 iOS デバイスは、Encryption Mode 3、Security Mode 4、および Service Level 1 の接続に対応しています。 iOS は以下の Bluetooth プロファイルをサポートしています。

- ハンズフリープロファイル （HFP）
- 電話帳アクセスプロファイル （PBAP）
- メッセージアクセスプロファイル （MAP）
- 高度オーディオ配信プロファイル （A2DP）
- オーディオ／ビデオリモートコントロールプロファイル （AVRCP）
- パーソナルエリアネットワークプロファイル （PAN）
- ヒューマンインターフェイスデバイスプロファイル （HID）

これらのプロファイルのサポートは、 デバイスによって異なります。

詳しくは、 support.apple.com/kb/ht3647 を参照してください。

シングルサインオン

iOS では、企業ネットワークへの認証にシングルサインオン（SSO）を使用できます。SSO は Kerberos ベースのネットワークに対応しており、アクセスが承認されているサービスに対してユーザを認証します。SSO は、幅広い範囲のネットワークアクティビティに利用することができ、「Safari」の安全なセッションや、他社製 App で使用できます。証明書ベースの認証（PKINIT）にも対応しています。

iOS の SSO は、SPNEGO トークンと HTTP Negotiate プロトコルを利用して、Kerberos ベースの認証ゲートウェイや、Kerberos チケットをサポートする統合 Windows 認証システムで動作します。SSO サポートは、オープンソースの Heimdal プロジェクトに基づいています。

以下の暗号化タイプがサポートされています。

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

「Safari」は SSO をサポートしています。また、標準の iOS ネットワーク API を使用する他社製 App も、SSO を使用するように構成できます。SSO を設定するために、iOS は構成プロファイルペイロードをサポートしており、これにより MDM ソリューションが必要な設定をプッシュできます。これには、ユーザのプリンシパル名（Active Directory ユーザアカウント）の設定や Kerberos 領域設定、SSO の使用を許可する App と「Safari」の Web URL の設定が含まれます。

連係機能

連係機能では、iCloud、Bluetooth、Wi-Fi といったテクノロジーを利用することで、使用するデバイスを変更してもアクティビティを継続できます。連係機能、電話の発着信、テキストメッセージの送受信、モバイルデータ通信によるインターネット接続の共有などに利用できます。

Handoff

Handoff を使用すると、ユーザの Mac と iOS デバイスが近くにあるとき、作業中のあらゆる項目を一方のデバイスから他方のデバイスに自動的に渡すことができます。これにより、ユーザはデバイスを切り替えてすぐに作業を再開できます。

Handoff に対応する別のデバイスでユーザが iCloud にサインインすると、2 つのデバイスが APNs を使用して Bluetooth Low Energy 4.2 の OOB（帯域外）ペアリングを確立します。個別のメッセージは iMessage と同様の方法で暗号化されます。デバイスがペアリングされると、各デバイスで 256 ビットの AES 対称鍵が生成され、デバイスのキーチェーンに保存されます。この鍵を使って Bluetooth Low Energy アドバタイズメントの暗号化と認証を行います。このアドバタイズメントでは、GCM モードの AES-256 を使用して、iCloud でペアリングされたほかのデバイスにアクティビティの現在の状態を伝達します。このとき、リプレイ攻撃に対する防御策が講じられます。

デバイスは、新しい鍵でのアドバタイズメントをはじめて受信すると、発信元のデバイスと Bluetooth Low Energy 接続を確立し、アドバタイズメントの暗号鍵を交換します。この接続は、Bluetooth Low Energy 4.2 の標準の暗号化によって保護され、個別のメッセージも iMessage と同様の方法で暗号化されます。特定の状況では、これらのメッセージが Bluetooth Low Energy ではなく APNs を介して送信されます。アクティビティのペイロードは、iMessage と同じ方法で保護および転送されます。

ネイティブ App と Web サイトの間での Handoff

Handoff を使用すると、iOS のネイティブ App で、その App のデベロッパが正当に制御しているドメインの Web ページの閲覧を再開できます。また、ネイティブ App でのユーザアクティビティを Web ブラウザで再開することもできます。

デベロッパが制御していない Web サイトの再開をネイティブ App が要求できないようにするため、App は再開する Web ドメインを正当に制御していることを示す必要があります。 Web サイトのドメインの制御は、 共有 Web 証明書のメカニズムによって確立されます。 詳しくは、この文書の「暗号化とデータ保護」 セクションの「保存済みパスワードへのアクセス」 を参照してください。 ユーザアクティビティの Handoff の受け入れを App に許可するには、 App がドメイン名を制御していることをシステムで検証する必要があります。

Web ページの Handoff は、 Handoff API を採用しているどのブラウザからも開始できます。ユーザが Web ページを表示すると、その Web ページのドメイン名が、暗号化された Handoff アドバタイズメントバイトでアドバタイズされます。 このアドバタイズメントバイトは、このセクションで前述したように、 同じユーザのほかのデバイスでのみ復号できます。

Handoff を受け取るデバイスでは、 アドバタイズされたドメイン名からの Handoff をインストール済みのネイティブ App が受け入れたことが検知され、 そのネイティブ App のアイコンが Handoff のオプションとして表示されます。 そのネイティブ App は、 起動後に Web ページの完全な URL とタイトルを受け取ります。 それ以外の情報はブラウザからネイティブ App に渡されません。

また、 Handoff を受け取るデバイスに同じネイティブ App がインストールされていないときのために、 ネイティブ App はフォールバック URL を指定できます。 その場合は、 ユーザのデフォルトブラウザが Handoff の App オプションとして表示されます（そのブラウザが Handoff API を採用している場合）。 Handoff が要求されるとブラウザが起動し、 受け渡し側の App から提供されたフォールバック URL を開きます。 このフォールバック URL には、 ネイティブ App のデベロッパが制御しているドメイン名のみに制限されるという要件はありません。

サイズが大きいデータの Handoff

一部の App では、Handoff の基本機能に加え、Apple 製のピアツーピア Wi-Fi テクノロジーによるサイズの大きいデータの送信機能（AirDrop と同様の方法で行われます）をサポートする API が使用されることがあります。 たとえば、「メール」 App では、 サイズが大きい添付ファイルが含まれるメールの下書きで Handoff をサポートするために、それらの API が使用されます。

App でこの機能が使用されると、 2 つのデバイス間で通常の Handoff とまったく同じように受け渡しが開始されます（前のセクションを参照）。 ただし、 受け取るデバイスは、 Bluetooth Low Energy を使用して最初のペイロードを受信した後で、 Wi-Fi で新しい接続を開始します。この接続は暗号化され（TLS）、iCloud 識別情報の証明書が交換されます。 証明書内の識別情報がユーザの識別情報と照合されて確認されます。 それ以降のペイロードデータは、 転送が完了するまで、 この暗号化された接続で送信されます。

ユニバーサルクリップボード

ユニバーサルクリップボードでは、 Handoff を活用してユーザのクリップボードの内容をデバイス間で安全に転送できるので、 1 台のデバイスでコピーした内容を別のデバイスでペーストできます。クリップボードの内容はほかの Handoff データと同様に保護され、 App のデベロッパが共有を禁止していない限り、 デフォルトでユニバーサルクリップボードと共有されます。

App はユーザがクリップボードの内容をその App にペーストしたかどうかにかかわらず、 クリップボードのデータにアクセスできます。 ユニバーサルクリップボードを使用すると、このデータアクセス範囲が、 ユーザのほかのデバイス（iCloud へのサインインによって決まります）で実行されている App に拡張されます。

自動ロック解除

自動ロック解除をサポートする Mac コンピュータでは、 Bluetooth Low Energy とピアツーピア Wi-Fi を使うことで、 ユーザの Apple Watch で安全に Mac のロックを解除できます。この機能に対応し、 同じ iCloud アカウントに関連付けられている各 Mac と Apple Watch では、 2 ファクタ認証（TFA）を使用する必要があります。

Apple Watch による Mac のロック解除を有効にすると、 自動ロック解除 ID を使用する安全なリンクが確立されます。 Mac はランダムなワンタイムロック解除シークレットを作成し、 安全なリンクを介して Apple Watch に送信します。 このシークレットは Apple Watch 上に保存され、

Apple Watch のロックが解除されているときにのみアクセスできます（「暗号化とデータ保護」セクションの「データ保護クラス」を参照）。この新しいシークレットは、ユーザのパスワードとは異なります。

ロック解除を処理するときは、Mac が Bluetooth Low Energy を使用して Apple Watch への接続を作成します。その後、2 台のデバイス間で安全なリンクが確立されます。この際、安全なリンクが最初に有効になったときに使用された共有鍵が使用されます。次に Mac と Apple Watch が、ピアツーピア Wi-Fi と安全なリンクから導出された安全な鍵を使用して、2 台のデバイス間の距離を特定します。デバイス間の距離が一定範囲内の場合は、共有済みのシークレットが安全なリンクで転送され、Mac のロックが解除されます。ロック解除が正常に行われると、Mac が現在のロック解除シークレットを新しいワンタイムロック解除シークレットに置き換え、安全なリンクを介して新しいロック解除シークレットを Apple Watch に送信します。

iPhone 経由の通話

Mac、iPad、または iPod touch が iPhone と同じ Wi-Fi ネットワークに接続されている場合、これらのデバイスは iPhone の携帯電話接続を利用して通話を発信／着信できます。この構成には、これらのデバイスが同じ Apple ID アカウントで iCloud と FaceTime の両方にサインインしている必要があります。

電話の着信があると、**Apple プッシュ通知サービス（APNs）**によって、構成済みのすべてのデバイスに通知されます。すべての通知で iMessage と同じエンドツーエンドの暗号化が使用されます。同じネットワーク上にあるデバイスに、電話の着信を通知する UI が表示されます。電話に出ると、2 つのデバイス間の安全なピアツーピア接続を使用して、ユーザの iPhone から音声がシームレスに転送されます。

1 台のデバイスで着信に応答すると、Bluetooth Low Energy 経由で簡潔にアドバタイズすることで、iCloud でペアリングされた近くにあるデバイスの着信音が停止します。アドバタイズメントバイトは、Handoff アドバタイズメントと同じ方法で暗号化されます。

電話の発信も Apple プッシュ通知サービス経由で iPhone に転送されます。オーディオも同様にデバイス間の安全なピアツーピアリンクを介して転送されます。

iPhone 経由の通話は、「FaceTime」設定の「iPhone での通話」をオフにすることで通話のリレーを無効にできます。

iPhone の SMS/MMS 転送

SMS/MMS 転送では、iPhone で受信した SMS テキストメッセージを、ユーザが登録した iPad、iPod touch、Mac に自動的に送信します。各デバイスで同じ Apple ID アカウントを使って iMessage サービスにサインインする必要があります。2 ファクタ認証が有効な場合は、SMS/MMS 転送を有効にすると、信頼されるユーザのデバイスがすべて自動的に登録されます。それ以外の場合は、iPhone によって生成されるランダムな 6 桁の数字のコードを入力することで、各デバイスで登録が検証されます。

デバイスがリンクされると、iPhone はこのセクションの「iMessage」で説明されている方法で、着信した SMS テキストメッセージを暗号化し、各デバイスに転送します。返信は同じ方法で iPhone に送り返されてから、iPhone がその返信をテキストメッセージとして通信事業者の SMS 送信システムを使って送信します。SMS/MMS 転送は、「メッセージ」の設定でオン／オフを切り替えられます。

Instant Hotspot

Instant Hotspot をサポートする iOS デバイスでは、Bluetooth Low Energy を使用して、同じ iCloud アカウントにサインインしているデバイスを検出し、通信します。OS X Yosemite 以降を搭載し、互換性のある Mac も、同じテクノロジーを使用して Instant Hotspot 対応の iOS デバイスを検出し、通信します。

ユーザが iOS デバイスで「Wi-Fi」設定を開くと、そのデバイスは同じ iCloud アカウントにサインインしているすべてのデバイスが合意した識別子を含む Bluetooth Low Energy アドバタイズメントを発信します。この識別子は iCloud アカウントに関連付けられた DSID（Destination Signaling Identifier）から生成され、定期的に入れ替えられます。同じ

iCloud アカウントにサインインしているほかのデバイスがすぐ近くにあり、インターネット共有に対応している場合、それらのデバイスは信号を検出して応答し、デバイスが使用可能であることを示します。

ユーザがインターネット共有に使用できるデバイスを選択すると、インターネット共有をオンにするリクエストがそのデバイスに送信されます。このリクエストは、Bluetooth Low Energy の標準の暗号化を使用して暗号化されたリンクで送信され、リクエスト自体も iMessage と同様の方法で暗号化されます。その後、デバイスは、同様に各メッセージを暗号化し、同じ Bluetooth Low Energy リンクを介して、インターネット共有の接続情報を含む応答を返します。

AirDrop のセキュリティ

AirDrop をサポートする iOS デバイスは、Bluetooth Low Energy（BLE）と Apple 製のピアツーピア Wi-Fi テクノロジーを使用して、OS X 10.11 以降を搭載する AirDrop 対応 Mac コンピュータなどの近くのデバイスにファイルや情報を送信できます。Wi-Fi 通信を使用して、インターネット接続や Wi-Fi アクセスポイントを使用せずにデバイス間で直接通信します。

ユーザが AirDrop を有効にすると、2048 ビットの RSA 識別情報がデバイスに保存されます。また、ユーザの Apple ID に関連付けられているメールアドレスと電話番号を基に、AirDrop 識別情報のハッシュが作成されます。

ユーザが項目の共有方法として AirDrop を選択すると、デバイスが Bluetooth Low Energy 経由で AirDrop 信号を発信します。スリープが解除され AirDrop がオンになっている別のデバイスが近くにあり、そのデバイスがこの信号を検出すると、所有者の識別情報のハッシュの短縮バージョンを使って応答します。

AirDrop は、デフォルトでは「連絡先のみ」と共有するように設定されています。AirDrop を使ってすべての人と共有することも、この機能を完全にオフにすることもできます。「連絡先のみ」モードでは、AirDrop を開始した送信デバイスが識別情報のハッシュを受信すると、そのハッシュを「連絡先」App の登録者のハッシュと照合します。一致が見つかると送信デバイスがピアツーピア Wi-Fi ネットワークを作成し、Bonjour 経由で AirDrop 接続をアドバタイズします。受信デバイスはこの接続を使って、識別情報の完全なハッシュをイニシエータに送信します。完全なハッシュ値も「連絡先」内の情報と一致した場合は、受信者の下の名前と写真（「連絡先」にある場合）が AirDrop の共有シートに表示されます。

AirDrop を使用するときは、送信ユーザが共有したい相手を選択します。送信デバイスが、暗号化された（TLS）接続を受信デバイスと開始し、そこで iCloud 識別情報の証明書が交換されます。証明書内の識別情報は、お互いのユーザの「連絡先」を使って照合および検証されます。その後、受信ユーザは、識別情報が確認されたユーザまたはデバイスからの受信データの承諾を求められます。複数の受信者が選択された場合は、このプロセスが送信先ごとに繰り返されます。

「すべての人」モードでも同じプロセスが使用されますが、「連絡先」で一致が見つからなかった場合、AirDrop の送信シートには受信デバイスのシルエットとデバイス名（「設定」＞「一般」＞「情報」＞「名前」で定義）が表示されます。

組織は、MDM ソリューションによって管理されているデバイスまたは App で AirDrop の使用を制限できます。

Wi-Fi パスワードの共有

Wi-Fi パスワードの共有をサポートする iOS デバイスでは、AirDrop と同様の仕組みを利用して、デバイス間で Wi-Fi パスワードを送信できます。

ユーザが Wi-Fi ネットワークを選択して（リクエスト側） Wi-Fi パスワードを求められると、Apple デバイスは Wi-Fi パスワードが必要であることを示す Bluetooth Low Energy アドバタイズメントを開始します。 スリープが解除され、目的の Wi-Fi ネットワークのパスワードを持っている別のデバイスが近くにある場合、 そのデバイスは Bluetooth Low Energy を使用してリクエスト側のデバイスに接続します。

Wi-Fi パスワードを持っているデバイス（付与側） には、 リクエスト側の連絡先情報が必要です。 また、 リクエスト側は、 AirDrop と同様の仕組みを使って自らの識別情報を証明する必要があります。 識別情報が証明されると、 付与側がリクエスト側に 64 文字の PSK を送信します。 これはネットワークへの接続にも使用できます。

組織は、 MDM ソリューションによって管理されているデバイスまたは App で Wi-Fi パスワードの共有の使用を制限できます。

Apple Pay

Apple Pay を使えば、 サポートされている iOS デバイス、 Apple Watch、 および Mac で、 プライバシーを守りながら、 店舗や App 内、「Safari」で開いた Web サイト上で簡単かつ安全に支払いを行えます。Apple Pay 対応の交通系 IC カードを「Wallet」に追加することもできます。 ユーザにとって使いやすいだけでなく、 ハードウェアとソフトウェアの両面でセキュリティが統合されています。

Apple Pay は、 ユーザの個人情報を保護できるように設計されており、 ユーザが特定される可能性のあるトランザクション情報を一切収集しません。 支払いトランザクションは、 ユーザ、 加盟店、 およびカード発行会社間でのみ行われます。

Apple Pay のコンポーネント

Secure Element：Secure Element は、 Java Card プラットフォームを実行する業界標準の認定チップで、 電子決済に対する金融業界の要件に準拠しています。

NFC コントローラ：NFC コントローラは、 Near Field Communication（NFC）プロトコルをサポートし、 アプリケーションプロセッサと Secure Element 間、 および Secure Element と POS 端末間の情報を転送します。

Wallet：「Wallet」 は、 クレジットカード、 デビットカード、 店舗カードの追加と管理、 および Apple Pay による支払いに使用されます。 ユーザは 「Wallet」 で自分のカードを確認できます。 また、 カード発行会社が提供する追加情報 （カード発行会社のプライバシーポリシー、 最近の取引明細など） を確認できる場合もあります。 以下の場所で Apple Pay にカードを追加することもできます。

- iOS の設定アシスタントと「設定」
- Apple Watch 用の「Watch」 App
- Mac の「Wallet と Apple Pay」 システム環境設定パネル

また、「Wallet」 に交通系 IC カード、 ポイントカード、 搭乗券、 チケット、 ギフトカード、 学生証などを追加して管理することもできます。

Secure Enclave：iPhone、 iPad、 Apple Watch では、 Secure Enclave がその認証プロセスを管理し、 支払いトランザクションの続行を許可します。

Apple Watch では、 デバイスのロックを解除し、 サイドボタンをダブルクリックする必要があります。 ダブルクリックが検出されると、 その情報はアプリケーションプロセッサを経由せず、 Secure Element または利用可能な場合は Secure Enclave に直接渡されます。

Apple Pay サーバ：Apple Pay サーバは、「Wallet」 のクレジットカード、 デビットカード、 交通系 IC カード、 学生証の設定やプロビジョニングのほかに、 Secure Element に格納されているデバイスアカウント番号も管理します。 また、 デバイスとペイメントネットワークまたはカード発行会社のサーバの双方と通信します。 さらに、 App 内での支払いに使用する支払い資格情報の再暗号化も行います。

Apple Pay が Secure Element を利用する方法

Secure Element では、 Apple Pay を管理するために特別に設計されたアプレットをホストしています。 また、 ペイメントネットワークやカード発行会社によって認定されたアプレットも含まれています。 クレジットカード、 デビットカード、 プリペイドカードのデータは、 ペイメントネットワークまたはカード発行会社からこれらのアプレットに送信されますが、 その際、 ペイメントネットワークまたはカード発行会社とアプレットのセキュリティドメインしか知らない鍵によって暗号化されます。 このデータはアプレット内に保存され、 Secure Element のセキュリティ機能を使って保護されます。 トランザクションの実行中、 決済用端末は専用のハードウェアバスを使用して Near Field Communication（NFC）コントローラ経由で Secure Element と直接通信します。

Apple Pay が NFC コントローラを利用する方法

NFC コントローラは Secure Element へのゲートウェイとして機能し、 これにより、 すべての非接触型支払いトランザクションが、 デバイスの近くにある POS 端末により実行されることが保証されます。 フィールド範囲内の端末から届いた支払い要求のみが、 NFC コントローラによって非接触型トランザクションとしてマークされて処理されます。

カード保持者が Touch ID、 Face ID、 またはパスコードを使用するか、 あるいはロック解除された Apple Watch でサイドボタンをダブルクリックして、 クレジットカード、 デビットカード、 プリペイドカード（店舗カードを含む）での支払いを承認すると、 Secure Element 内のペイメントアプレットが作成した非接触型の応答がコントローラによって排他的に NFC フィールドに配信されます。 その結果、 非接触型支払いトランザクションの支払い承認の詳細情報は、 ローカルの NFC フィールド範囲内に留まり、 アプリケーションプロセッサに開示されることは決してありません。 これに対し、 App 内および Web 上での支払い承認の詳細情報はアプリケーションプロセッサに配信されます。 ただし、 Apple Pay サーバへの配信前に必ず Secure Element によって暗号化されます。

クレジットカード、 デビットカード、 プリペイドカードのプロビジョニング

ユーザがクレジットカード、 デビットカード、 プリペイドカード（店舗カードを含む）を「Wallet」に追加すると、 Apple によって、 そのカード情報とユーザのアカウントおよびデバイスに関するその他の情報が、 該当するカード発行会社またはカード発行会社認定のサービスプロバイダに安全に送信されます。 カード発行会社はこの情報を使って、 そのカードの「Wallet」への追加を承認するかどうかを決定します。

Apple Pay は、 カードのプロビジョニングプロセスの一部として、「**Required Fields**」、「**Check Card**」、「**Link and Provision**」という 3 つのサーバ側呼び出しを使用して、 カード発行会社またはネットワークとデータの送受信を行います：カード発行会社またはネットワークはこれらの呼び出しを使用して、 カードの確認、 承認、 および「Wallet」への追加を行います。 これらのクライアントサーバセッションは TLS v1.2 を使って暗号化されます。

完全なカード番号は、 デバイスにも Apple のサーバにも保存されません。 その代わりに、 デバイスアカウント番号が一意に作成され、 暗号化された後に Secure Element に保存されます。 この一意のデバイスアカウント番号は、 Apple でもアクセスできない方法で暗号化されます。 このデバイスアカウント番号は、 通常のクレジットカードやデビットカードの番号とは異なるため、 カード発行会社またはペイメントネットワーク側は、 クレジットカードやデビットカードの番号を磁気ストライプカード、 電話、 Web サイトなどで悪用されないように保護できます。 Secure Element 内のデバイスアカウント番号は iOS および watchOS から切り離されており、 Apple のサーバに保存されることは決してありません。 また、 iCloud にバックアップされることもありません。

Apple Watch で使用するカードを登録するには、 iPhone の「Watch」App またはカード発行会社が提供する iPhone App を使用します。 Apple Watch にカードを追加するには、 その Apple Watch が Bluetooth の通信範囲内にある必要があります。 カードは Apple Watch で使用するために登録され、 独自のデバイスアカウント番号を持ちます。 デバイスアカウント番号は、 Apple Watch の Secure Element 内に格納されます。

追加されたクレジットカード、 デビットカード、 プリペイドカード （店舗カードを含む） は、 同じ iCloud アカウントにサインインしているデバイスで設定アシスタントを実行したときにカードのリストに表示されます。 これらのカードは、 少なくとも 1 つのデバイスで有効になっている限りこのリストに表示されます。すべてのデバイスから削除されて 7 日以上経つと、このリストからも削除されます。この機能を有効にするには、 それぞれの iCloud アカウントで 2 ファクタ認証を有効にする必要があります。

クレジットカードまたはデビットカードを手動で Apple Pay に追加する

カードを手動で追加する場合は、プロビジョニングプロセスを円滑に処理するため、名義、カード番号、有効期限、および CVV を使用します。「設定」、「Wallet」 App、または 「Watch」 App で、それらの情報を手入力するか、 デバイスのカメラを使用して入力できます。 カメラでカード情報を取り込む場合は、 Apple により名義、 カード番号、 有効期限の取得が試みられます。 写真がデバイスやフォトライブラリに保存されることはありません。 必要な情報がすべて入力されると、 Check Card プロセスが CVV 以外の各フィールドを確認します。 情報は暗号化されて Apple Pay サーバに送信されます。

Check Card プロセスから利用条件 ID が返されたら、 Apple はカード発行会社の利用条件をダウンロードしてユーザに表示します。 ユーザが利用条件に同意すると、 Apple は同意を得た利用条件の ID および CVV を Link and Provision プロセスに送信します。 このほか、 Link and Provision プロセスの一部として Apple は、 デバイスからの情報をカード発行会社またはネットワークと共有します。 具体的には、 iTunes と App Store のアカウント利用に関する情報 (iTunes での長期間のトランザクションがあるかどうかなど)、 デバイスに関する情報 （電話番号、デバイスの名前とモデル、Apple Pay の設定に必要なペアリング相手の iOS デバイスなど)、カードを追加したときのおおよその位置情報 （「位置情報サービス」 を有効にしている場合） などです。カード発行会社はこの情報を使って、 そのカードの Apple Pay への追加を承認するかどうかを決定します。

Link and Provision プロセスの結果として以下の 2 つの処理が実行されます。

- デバイスが、 クレジットカードまたはデビットカードを表す 「Wallet」 パスファイルのダウンロードを開始する。
- デバイスが、 当該カードの Secure Element へのバインドを開始する。

パスファイルには、 カードのデザインや連絡先情報、 関連するカード発行会社の App、 サポートされる機能などのカードに関するメタデータをダウンロードするための URL が含まれています。 ほかにも、 Secure Element のパーソナライズが完了したかどうか、 カード発行会社によってカードが利用停止になっていないかどうか、 Apple Pay で支払いを行うためにカードで追加の検証が必要かどうかなど、 パスの状態に関する情報も含まれています。

iTunes Store アカウントからクレジットカードまたはデビットカードを Apple Pay に追加する

「iTunes」 に登録されているクレジットカードやデビットカードの場合、 ユーザは Apple ID パスワードの再入力を求められることがあります。 カード番号が 「iTunes」 から取得され、 Check Card プロセスが開始されます。 そのカードが Apple Pay に対応している場合は、 利用条件がダウンロードされてデバイスに表示されます。 その後、 利用条件の ID とカードのセキュリティコードが Link and Provision プロセスに送られます。 登録されている iTunes アカウントのカードには追加の検証が必要な場合があります。

カード発行会社の App からクレジットカードまたはデビットカードを追加する

App が Apple Pay で使用できるよう登録されている場合は、その App とカード発行会社のサーバ用の鍵が生成されます。 これらの鍵はカード発行会社に送信されるカード情報の暗号化に使用されます。 これによって、 iOS デバイスがカード情報を読み取ることができなくなります。 プロビジョニングプロセスは、 上記の手動でカードを追加する場合と同じように行われますが、 CVV の代わりにワンタイムパスワードが使用されます。

追加の検証

カード発行会社は、クレジットカードまたはデビットカードに追加の検証が必要かどうかを決定できます。カード発行会社から提供されるサービス内容によりますが、テキストメッセージ、メール、カスタマーサービスとの通話、承認された他社製 App 内で提供される方法など、追加の検証を行う方法をユーザがさまざまなオプションから選択できる場合があります。テキストメッセージやメールの場合は、カード発行会社に登録されている連絡先情報からユーザが選択します。そこにコードが送信されるので、そのコードを「Wallet」、「設定」、または「Watch」App に入力する必要があります。カスタマーサービスや App を使用する検証の場合は、カード発行会社が独自の方法で実施します。

支払い承認

Secure Enclave が搭載されたデバイスでは、Secure Element は Secure Enclave から承認を受けた後にのみ支払いを許可します。この際、iPhone または iPad では、ユーザが Touch ID、Face ID、またはデバイスパスコードで認証したことを確認します。利用できる場合には Touch ID または Face ID がデフォルトの方法ですが、パスコードもいつでも使用できます。指紋の認証に 3 回失敗するか、顔の認証に 2 回失敗すると自動的にパスコードが使用できるようになり、5 回失敗するとパスコードが必須になります。Touch ID または Face ID が設定されていないか、Apple Pay に対して有効になっていない場合もパスコードが要求されます。Apple Watch で支払いを実行するには、パスコードでデバイスのロックを解除し、サイドボタンをダブルクリックする必要があります。

Secure Enclave と Secure Element 間の通信はシリアルインターフェイス経由で行われます。Secure Element が NFC コントローラに接続され、そこからアプリケーションプロセッサに接続されます。Secure Enclave と Secure Element は直接接続されてはいませんが、製造工程で書き込まれた共有ペアリングキーを使用することで安全に通信できます。通信の暗号化と認証は AES に基づくもので、通信の両側でノンスを使うことでリプレイ攻撃から保護します。ペアリングキーは、Secure Enclave の UID キーと Secure Element の一意の識別子から、Secure Enclave 内で生成されます。生成されたペアリングキーは、製造時に Secure Enclave から **HSM（ハードウェア・セキュリティ・モジュール）** に安全に転送されます。HSM には、その後にペアリングキーを Secure Element に導入するのに必要なキーマテリアルが用意されています。

ユーザがトランザクションを承認すると、認証の種類およびトランザクションの種類（非接触型または App 内）の詳細に関する署名済みデータが AR（Authorization Random）値に付加されて、Secure Enclave から Secure Element に送信されます。AR は、ユーザがはじめてクレジットカードをプロビジョニングしたときに Secure Enclave 内で生成されます。これは、Apple Pay が有効な間は維持され、Secure Enclave の暗号化およびロールバック防止メカニズムによって保護されます。AR は、ペアリングキーを使って Secure Element に安全に配信されます。Secure Element は、新しい AR 値を受け取ると、以前に追加されたすべてのカードに削除済みのマークを付けます。

Secure Element に追加されたクレジットカード、デビットカード、プリペイドカードは、カード追加時と同じペアリングキーの AR 値を使った承認が Secure Element に提示されない限り、使用できません。これにより以下のような状況の場合に、iOS から Secure Enclave に対して、AR のコピーに無効のマークを付けてカードを使用不可とするように指示することができます。

- パスコードがオフになった。
- ユーザが iCloud からサインアウトした。
- ユーザが「すべてのコンテンツと設定を消去」を選択した。
- デバイスがリカバリモードから復元された。

Apple Watch では、以下の場合にカードが無効とマークされます。

- Apple Watch のパスコードがオフになった。
- Apple Watch が iPhone からペアリング解除された。

Secure Element は、 ペアリングキーと現在の AR 値のコピーを使用して Secure Enclave から受け取った承認を検証してから、 非接触型支払いを行うペイメントアプレットを有効にします。 このプロセスは、 App 内トランザクションで、 暗号化された支払いデータをペイメントアプレットから取得する場合にも適用されます。

トランザクション固有のダイナミック・セキュリティ・コード

ペイメントアプレットから送信される支払いトランザクションには、 デバイスアカウント番号に加えて支払い用クリプトグラムが含まれています。 このクリプトグラムは 1 回限りのコードで、 新しいトランザクションが発生するたびに増分されるトランザクションカウンタと、 パーソナライズ時にペイメントアプレットでプロビジョニングされる鍵を使って計算され、 ペイメントネットワークとカード発行会社の両方またはいずれかに通知されます。 支払い方式によっては、 この計算に以下のようなデータも使用されます。

- 端末で生成される予測不可能な番号 （NFC トランザクションの場合）。
- Apple Pay サーバのノンス （App 内トランザクションの場合）。

これらのセキュリティコードはペイメントネットワークとカード発行会社に送信され、 各トランザクションの検証に使用されます。 セキュリティコードの長さは、 実行中のトランザクションの種類によって異なることがあります。

店舗でのクレジットカードまたはデビットカードによる支払い

動作中の iPhone が NFC フィールドを検出すると、 要求されたカード （そのカードで自動選択がオンになっている場合）、 または「設定」で管理されているメインカードがユーザに表示されます。 ユーザは、「Wallet」 App でカードを選択することもできます。 デバイスがロックされている場合は、 以下の操作を行います。

- Touch ID 搭載デバイスではホームボタンをダブルクリックする
- Face ID 搭載デバイスではサイドボタンをダブルクリックする DD

次に、 ユーザは Touch ID、 Face ID、 またはパスコードを使用して認証する必要があります。 その後、 支払い情報が転送されます。 Apple Watch では、 ロックが解除されているときにサイドボタンをダブルクリックすると、 支払い用のメインカードが有効になります。 ユーザの認証がない限り、 支払い情報は送信されません。

ユーザが認証すると、 デバイスアカウント番号とトランザクション固有のダイナミック・セキュリティ・コードを使って支払いが処理されます。 クレジットカードまたはデビットカードの実際の番号全体が、 Apple やユーザのデバイスから加盟店に送信されることはありません。 Apple は、 トランザクションのおおよその時間や場所といったトランザクション情報を、 匿名で受け取る場合があります。 これは、 Apple Pay やその他の Apple の製品およびサービスの改善に利用されます。

App 内でのクレジットカードまたはデビットカードによる支払い

Apple Pay は、 iOS App や Apple Watch App 内での支払いにも使用できます。 ユーザが Apple Pay を利用して App 内で支払うと、 Apple は、 暗号化されたトランザクション情報を受信し、 それをデベロッパ固有の鍵を使って再暗号化してから、 デベロッパまたは加盟店に送信します。 Apple Pay には、 おおよその購入金額などが匿名のトランザクション情報として保持されます。 この情報によってユーザを特定することはできず、 ユーザの購入内容がこの情報に含まれることは決してありません。

App が Apple Pay の支払いトランザクションを開始すると、 デバイスからの暗号化されたトランザクションは、 加盟店よりも前に Apple Pay サーバに送信されます。 Apple Pay サーバがそのトランザクションを受信すると、 加盟店固有の鍵を使って再暗号化した後、 加盟店に転送します。

App が支払いを要求する場合、その App は API を呼び出して、デバイスが Apple Pay に対応しているかどうか、および加盟店が対応しているペイメントネットワーク上で支払い可能なクレジットカードまたはデビットカードをユーザが保持しているかどうかを調べます。App は、請求先住所、出荷先住所、連絡先情報など、トランザクションの処理および完了に必要となるすべての情報を要求します。次に App は、Apple Pay シートの表示を iOS に依頼します。Apple Pay シートは、App の情報と使用するカードなど、ほかの必要な情報を要求します。

この時点で App には、最終的な送料を計算するための市区町村、都道府県、郵便番号の情報が通知されます。要求したすべての情報が App に提供されるのは、ユーザが Touch ID、Face ID、またはデバイスパスコードで支払いを承認した後です。支払いが承認されると、Apple Pay シートで提供された情報が加盟店に転送されます。

ユーザが支払いを承認すると、ノンスを取得するための呼び出しが Apple Pay サーバに対して行われます。ノンスは、店舗でのトランザクションで使用する NFC 端末から返される値と同様の働きをします。ノンスは、ほかのトランザクションデータと共に Secure Element に渡されます。そこで支払い資格情報が生成され、Apple の鍵を使用して暗号化されます。暗号化された支払い資格情報は、Secure Element から Apple Pay サーバに渡されます。Apple Pay サーバは資格情報を復号し、資格情報内のノンスと Apple Pay サーバからあらかじめ送信されたノンスとを照合してから、加盟店 ID と関連付けられた加盟店キーを使って支払い資格情報を再暗号化します。その後、支払い資格情報はデバイスに返され、さらに API 経由で App に戻されます。App がその情報を受け取ったら、それを加盟店のシステムに送信して処理に進みます。加盟店は、支払い資格情報を自分の秘密鍵で復号して処理を行います。この仕組みを利用し、さらに Apple のサーバからの署名を使うことで、加盟店は、そのトランザクションがこの特定の加盟店に向けられたものであることを確認できます。

API には、サポートされる加盟店 ID を指定するエンタイトルメントが必要です。また、トランザクションがほかの顧客に向けて処理されないように、App で注文番号や顧客 ID などのデータを追加し、Secure Element に送信して署名させることも可能です。これを行うには、App デベロッパが PKPaymentRequest で applicationData を指定します。このデータのハッシュが、暗号化された支払いデータに含められます。その後、加盟店は、自分の applicationData ハッシュが、支払いデータに含まれているものと一致することを確認する必要があります。

Web でのクレジットカードまたはデビットカードによる支払い

Apple Pay は、iOS デバイス、Apple Watch、および Mac から Web サイトで支払いを行うときにも使用できます。Apple Pay のトランザクションを Mac で開始し、同じ iCloud アカウントを使用して Apple Pay 対応 iPhone または Apple Watch でトランザクションを完了することもできます。

Web 上で Apple Pay を提供するすべての Web サイトが、Apple に登録する必要があります。Apple サーバがドメイン名検証を実行し、TLS クライアント証明書を発行します。Apple Pay をサポートする Web サイトは、HTTPS 経由でコンテンツを提供する必要があります。支払いトランザクションごとに、Web サイトは Apple が発行した TLS クライアント証明書を使用して、Apple サーバとの安全な一意の加盟店セッションを取得する必要があります。加盟店セッションデータは Apple によって署名されます。加盟店セッションの署名が検証されると、Web サイトはユーザが Apple Pay 対応デバイスを持っているかどうか、またユーザがそのデバイスでクレジットカード、デビットカード、プリペイドカードを有効にしているかどうかを照会できます。そのほかの詳細情報は共有されません。ユーザがこの情報を共有したくない場合は、iOS と macOS の「Safari」のプライバシー設定で Apple Pay 照会の機能を無効にできます。

加盟店セッションが検証されると、すべてのセキュリティおよびプライバシー対策は App 内での支払いの場合と同じになります。

Mac から iPhone または Apple Watch に Handoff する場合、Apple Pay はエンドツーエンドで暗号化された Apple Identity Service（IDS）プロトコルを使用して支払い関連情報をユーザの Mac から認証側デバイスに転送します。IDS はユーザのデバイスキーを使用して暗号化を実行するため、ほかのデバイスはこの情報を復号できず、Apple もこのキーを使うことはで

きません。 Apple Pay を Handoff するためのデバイス検出には、いくつかのメタデータと一緒にユーザのクレジットカードの種類と一意識別子が含まれます。 ユーザのカードに割り当てられているデバイス固有のアカウント番号は共有されず、ユーザの iPhone または Apple Watch で安全に保管された状態で維持されます。 また、Apple は iCloud キーチェーンを通じて、ユーザが最近使用した連絡先情報、出荷先住所、請求先住所を安全に転送します。

ユーザが Touch ID、Face ID、またはパスコードを使用するか、Apple Watch のサイドボタンをダブルクリックすることで支払いを承認すると、各 Web サイトの加盟店証明書に一意に暗号化されたペイメントトークンがユーザの iPhone または Apple Watch から Mac に安全に転送されてから、加盟店の Web サイトに送信されます。

互いの近くにあるデバイスのみが支払いを要求および完了できます。 近接性は Bluetooth Low Energy アドバタイズメントを通じて判定されます。

非接触型パス

「Wallet」は、対応パスから対応 NFC 端末にデータを送信できる VAS（Value Added Services）プロトコルに対応しています。 VAS プロトコルは非接触型端末に実装でき、NFC を使って対応する Apple デバイスと通信します。 VAS プロトコルは近距離で機能し、単独処理として、または Apple Pay トランザクションの一部として、非接触型パスを提示するために使用できます。

デバイスを NFC 端末に近付けると、端末では、パスの要求を送信することでパス情報の受信が開始されます。 ユーザが加盟店の識別子を含むパスを持っている場合、ユーザは Touch ID、Face ID、またはパスコードによるカード使用の承認を求められます。 パス情報、タイムスタンプ、および 1 回限りのランダムな ECDH P-256 鍵が加盟店の公開鍵と一緒に使用されてパスデータの暗号鍵が導出され、これが端末に送信されます。

ユーザはパスを手動で選択し、Touch ID、Face ID、またはパスコードで承認してから、加盟店の NFC 端末に提示することもできます。

Apple Pay Cash（日本未対応）

iOS 11.2 以降および watchOS 4.2 以降では、iPhone、iPad、または Apple Watch で Apple Pay を使って、ほかのユーザに送金したり、支払いを受けたり、請求したりできます。支払いを受けると、その金額が Apple Pay Cash アカウントに加算されます。 Apple Pay Cash アカウントには、「Wallet」からアクセスするか、ユーザが自分の Apple ID でサインインしている Apple Pay 対応デバイスの「設定」>「Wallet と Apple Pay」からアクセスできます。

個人間の送金や Apple Pay Cash を使用するには、ユーザが Apple Pay Cash 対応のデバイスで iCloud アカウントにサインインし、iCloud アカウントで 2 ファクタ認証を設定する必要があります。

Apple Pay Cash を設定すると、クレジットカードまたはデビットカードを追加したときと同じ情報が、Apple のパートナー銀行である Green Dot Bank と Apple の 100% 子会社である Apple Payments Inc. と共有されることがあります。 Apple Payments Inc. は、情報の保管と処理を Apple のほかの部署から切り離し、Apple のほかの部署に把握されない方法で行うことによってお客様のプライバシーを保護するために設立されました。 この情報はトラブルシューティング、不正防止、および法令順守の目的にのみ使用されます。

ユーザ間の請求と送金は、「メッセージ」App 内から、または Siri に依頼して開始します。 ユーザが送金を開始すると、iMessage に Apple Pay シートが表示されます。 常に Apple Pay Cash の残高が最初に使用されます。 必要に応じて、ユーザが「Wallet」に追加した第 2 のクレジットカードまたはデビットカードから不足分が引き出されます。

「Wallet」の Apple Pay Cash カードを Apple Pay で使用して、店舗、App、Web 上での支払いも行えます。Apple Pay Cash アカウントの残高は、銀行口座にも送金できます。別のユーザから支払いを受けるだけでなく、「Wallet」のデビットカードまたはプリペイドカードから Apple Pay Cash アカウントに残高を追加することもできます。

トランザクションが完了すると、Apple Payments Inc. がトランザクションデータを保存します。この情報はトラブルシューティング、不正防止、および法令順守の目的に使用される場合があります。Apple Pay Cash カードで送金した相手、支払いを受けた相手、買い物をした場所が、Apple のほかの部署に把握されることはありません。

Apple Pay での送金、Apple Pay Cash アカウントへの残高追加、銀行口座への送金を行うと、ノンスを取得するための呼び出しが Apple Pay サーバに対して行われます。ノンスは、App 内で Apple Pay 用に返される値と同様の働きをします。ノンスは、支払い署名を生成するために、ほかのトランザクションデータと共に Secure Element に渡されます。支払い署名は Secure Element から Apple Pay サーバに渡されます。Apple Pay サーバは、支払い署名とノンスを使用してトランザクションの認証、完全性、および正確性を検証します。その後送金が実行され、トランザクションの完了が通知されます。

トランザクションで、Apple Pay Cash への残高追加、別のユーザへの送金、または Apple Pay Cash の残高不足による不足分の支払いにクレジットカードまたはデビットカードを使用した場合は、暗号化された支払い資格情報も生成され、Apple Pay サーバに送信されます。これは App 内および Web サイト上で Apple Pay に使用される資格情報と同様のものです。

Apple Pay Cash アカウントの残高が一定の金額を超えるか、通常と異なるアクティビティが検出されると、ユーザに自らの識別情報の確認が求められます。社会保障番号や質問への回答（たとえば以前に住んでいた町名の確認）など、ユーザの識別情報を確認するために提供される情報は Apple のパートナーに安全に送信され、パートナーの鍵を使って暗号化されます。Apple はこのデータを復号できません。

交通系 IC カード

中国と日本では、対応する iPhone および Apple Watch モデルで、対応する交通系 IC カードを「Wallet」に追加できます。これは、物理的なカードから「Wallet」のデジタルデータに残高や定期券を転送するか、交通系 IC カードの発行会社が提供する App で新しいカードを作成して「Wallet」に追加するという方法で行うことができます。交通系 IC カードを「Wallet」に追加すると、iPhone または Apple Watch を改札機にかざすだけで交通機関を利用できるようになります。日本では、Suica カードを支払いに使用することもできます。

追加した交通系 IC カードはユーザの iCloud アカウントに関連付けられます。ユーザが複数のカードを「Wallet」に追加すると、Apple または交通系 IC カードの発行会社がカード間でユーザの個人情報および関連するアカウント情報をリンクできる場合があります。たとえば、My Suica カードを無記名の Suica カードとリンクできます。交通系 IC カードとトランザクションは、階層化された暗号鍵のセットを使って保護されます。

物理的なカードから「Wallet」に残高が転送される処理では、カードのシリアル番号の識別桁を入力するよう求められます。また、カードの所有者であることを証明するための個人情報の入力を求められることもあります。たとえば、My Suica カードまたは定期券情報の入った Suica カードの場合は、生年月日を入力する必要があります。iPhone から Apple Watch にカードを転送するときは、転送中に両方のデバイスがオンラインである必要があります。

残高は、「Wallet」経由で、または交通系 IC カードの発行会社の App から、クレジットカードやプリペイドカードの残高を使ってチャージできます。Apple Pay 使用時に残高を再読み込みする際のセキュリティについては、この文書の「App 内でのクレジットカードまたはデビットカードによる支払い」セクションを参照してください。

交通系 IC カードの発行会社の App 内で行われる交通系 IC カードのプロビジョニングプロセスについては、この文書の「カード発行会社の App からクレジットカードまたはデビットカードを追加する」セクションを参照してください。

交通系 IC カードの発行会社は、物理的なカードへの認証と、ユーザが入力したデータの検証を行うために必要な暗号鍵を持っています。検証が完了すると、システムは Secure Element 用のデバイスアカウント番号を作成し、新しく追加されたカードに転送された残高を追加して「Wallet」で有効にすることができます。日本では、物理的なカードからのプロビジョニングが完了すると、その物理的な Suica カードは無効になります。

どの種類のプロビジョニングでも、終了後に、交通系 IC カードの残高が暗号化され、Secure Element 内の指定されたアプレットに保存されます。交通系カードの運用会社は、残高のトランザクションに関してカードデータの暗号演算を行うために必要な鍵を持っています。

ユーザはデフォルトでエクスプレスカードを利用できるので、Touch ID、Face ID、またはパスコードを必要とせず、シームレスに支払ったり交通機関を利用したりできます。エクスプレスモードが有効な場合、付近にある非接触型カードリーダーが、最近利用した駅、トランザクション履歴、追加の切符などの情報にアクセスできる場合があります。ユーザは「Wallet と Apple Pay」設定で「エクスプレスカード」を無効にすることで、Touch ID、Face ID、またはパスコードによる認証の要求を有効にすることができます。

Apple Pay のほかのカードと同様に、交通系 IC カードでは、ユーザが以下の方法で使用を一時停止したり削除したりできます。

- 「iPhone を探す」でデバイスをリモートで消去する
- 「iPhone を探す」で紛失モードを有効にする
- モバイルデバイス管理（MDM）のリモート・ワイプ・コマンドを実行する
- ユーザの Apple ID アカウントページからすべてのカードを削除する
- iCloud.com からすべてのカードを削除する
- Wallet からすべてのカードを削除する
- 発行会社の App でカードを削除する

Apple Pay サーバから交通系 IC カードの運用会社に、それらのカードを一時停止または無効にするよう通知されます。Suica カードの場合は、ユーザがデバイスの消去を試みたときにデバイスがオフラインになっていると、一部の端末ではそれらの Suica カードを日本時間の翌日午前 0:01 まで使用できる場合があります。中国の交通系 IC カードは、ユーザのデバイスがオフラインの場合、引き続き使用できます。

ユーザが交通系 IC カードを削除した場合は、同じ Apple ID でサインインしているデバイスにカードを再び追加することによって、その残高を回収できます。

Student ID card（日本未対応）

iOS 12 では、対応している大学の学生や教職員が学校の ID カードを「Wallet」に追加して、カードに対応した施設への出入りや支払いに利用できます。

ユーザは、ID カードの発行会社または学校が提供する App を使用して「Wallet」に ID カードを追加します。その際に行われる技術的なプロセスは、この文書の「カード発行会社の App からクレジットカードまたはデビットカードを追加する」セクションで説明している内容と同じです。また、発行に使用する App は、ID へのアクセスを保護するアカウントで 2 ファクタ認証をサポートする必要があります。1 枚のカードは、同じ Apple ID でサインインしている最大 2 台の対応 Apple デバイスで同時に設定できます。

「Wallet」に学生証を追加すると、エクスプレスモードがデフォルトでオンになります。エクスプレスモードの学生証は、Touch ID、Face ID、またはパスコードによる認証なしで対応端末と情報をやりとりできます。ユーザは、「Wallet」で Student ID card の前面に表示される「詳細」ボタンをタップすることで、エクスプレスモードをオフにしてこの機能を無効にできます。エクスプレスモードを再度有効にするときは、Touch ID、Face ID、またはパスコードが必要になります。

Student ID card は以下の方法で無効にするか削除することができます。

- 「iPhone を探す」でデバイスをリモートで消去する
- 「iPhone を探す」で紛失モードを有効にする
- モバイルデバイス管理（MDM）のリモート・ワイプ・コマンドを実行する
- ユーザの Apple ID アカウントページからすべてのカードを削除する
- iCloud.com からすべてのカードを削除する
- Wallet からすべてのカードを削除する
- 発行会社の App でカードを削除する

カードの一時停止、削除、消去

ユーザは、「iPhone を探す」でデバイスを紛失モードにすることにより、iPhone、iPad、および Apple Watch で Apple Pay の使用を一時停止することができます。また、「iPhone を探す」や iCloud.com を使用して、または「Wallet」を使ってデバイス上で直接、Apple Pay のカードを削除したり消去したりすることもできます。Apple Watch では、iCloud の設定、iPhone の「Watch」App、または Apple Watch で直接、カードを削除できます。デバイスがオフラインで、モバイルデータ通信ネットワークまたは Wi-Fi ネットワークに接続していない場合でも、デバイス上でカードを使って支払う機能は、カード発行会社または関連のペイメントネットワークによって使用を一時停止されるか Apple Pay から削除されるかします。ユーザは、カード発行会社に電話をかけて、カード使用の一時停止や Apple Pay からの削除を依頼することもできます。

また、ユーザが「すべてのコンテンツと設定を消去」または「iPhone を探す」を使用して、あるいは、リカバリモードでデバイスを復元することでデバイス全体を消去すると、iOS は Secure Element に対して、すべてのカードに削除済みのマークを付けるように指示します。これにより、カードはただちに使用できない状態に変更され、その後 Apple Pay サーバに接続すると、Secure Element からカードが完全に消去されます。それとは別に、Secure Enclave は、以前登録されたカードでそれ以降の支払い承認ができなくなるように AR に無効のマークを付けます。デバイスがオンラインのときに、デバイスは Apple Pay サーバへの接続を試み、Secure Element 内のすべてのカードを確実に消去します。

インターネットサービス

強力な Apple ID パスワードを作成する
Apple ID は、iCloud、FaceTime、iMessage などの多くのサービスに接続するために使用されます。 ユーザが強力なパスワードを作成できるように、 すべての新規アカウントで以下のパスワード属性が必須になっています。

- 8 文字以上
- 小文字を含む
- 大文字を含む
- 数字を含む
- 同一文字を 3 文字以上連続して使用しない
- アカウント名と同一の文字列を使用しない

Apple のデバイスには、 iMessage、FaceTime、Siri からの提案、iCloud、iCloud バックアップ、 iCloud キーチェーンなど、 ユーザの利便性や生産性を高めるのに役立つ強力なサービスのセットが組み込まれています。

これらのインターネットサービスが実現するセキュリティ上の設計目標は、 iOS のプラットフォーム全体で推進するものと共通です。 その目標には、 デバイス内であってもワイヤレスネットワーク経由の転送時であっても安全が確保されたデータ処理、 ユーザの個人情報の保護、 情報とサービスへの悪意のあるアクセスや不正アクセスなどの脅威からの保護が含まれます。 iOS の全体的な使いやすさを損なうことなく、 各サービスで独自の強力なセキュリティアーキテクチャが採用されています。

Apple ID

Apple ID は、 iCloud、 iMessage、 FaceTime、 iTunes Store、 Apple Books、 App Store などの Apple のサービスへのサインインに使用するアカウントです。 アカウントへの不正アクセスを防止するため、 ユーザがそれぞれの Apple ID を安全に保持することが重要です。 Apple はこれを支援するため、 強力なパスワードの設定を必須にしています。 パスワードは、 8 文字以上で英字と数字の両方を含んでいる必要があります。 また、 同一文字を 3 文字以上連続して使用したり、 よく使用されるパスワードを設定したりすることはできません。 このようなガイドラインを最低要件とし、 さらに多くの文字や英字句読点 （ピリオドなど） を追加してパスワードをより強力にすることが推奨されます。 ユーザは 3 つのセキュリティ質問を設定する必要もあります。 これらの質問は、アカウント情報を変更したり忘れてしまったパスワードをリセットしたりするときに、 所有者の識別情報の確認に使用されます。

Apple は、 パスワードや請求先情報が変更されたときや Apple ID が新しいデバイスでのサインインに使用されたときなど、 アカウントに重要な変更が加えられた場合にメールやプッシュ通知の送信も行います。 身に覚えのない変更が行われた場合、 ただちに Apple ID のパスワードを変更するようユーザを促します。

また、 ユーザアカウントを保護するためのさまざまなポリシーや手順も採用されています。 これには、 サインインの再試行回数やパスワードリセットの試行回数の制限、 発生した攻撃の特定に役立つ不正行為の積極的な監視が含まれ、 お客様のセキュリティに影響する可能性がある新しい情報に Apple が対応するため、 ポリシーも定期的に見直しています。

2 ファクタ認証

ユーザが自分のアカウントをさらに安全に保護できるようにするため、 Apple は 2 ファクタ認証を提供しています。 これによって Apple ID のセキュリティがさらに 1 段階強化され、 ほかの人にパスワードを知られてしまった場合でも、 アカウントの所有者だけが自分のアカウントにアクセスできるようになります。

2 ファクタ認証を使えば、 ユーザの iPhone、 iPad、 または Mac など、 信頼できるデバイスでのみユーザのアカウントにアクセスできるようになります。 新しいデバイスにはじめてサインインする場合は、 Apple ID のパスワードのほかに、 6 桁の確認コードという 2 つの情報の入力が必要になります。 コードは自動的にユーザの信頼できるデバイスに表示されるか、 信頼できる電話番号に送信され、 このコードを入力することで、 ユーザは新しいデバイスを信頼し、 安全にサインインできることを確認できます。 パスワードだけではユーザのアカウントにアクセスできなくなるため、2 ファクタ認証のおかげで、 ユーザの Apple ID のセキュリティと、 Apple に保管されるすべての個人情報のセキュリティが向上します。 iOS、 macOS、 tvOS、 watchOS、 および Apple の Web サイトで使用されている認証システムには、 2 ファクタ認証が直接組み込まれています。

2 ファクタ認証について詳しくは、 次の Web サイトを参照してください。
support.apple.com/HT204915

2 ステップ確認

2013 年より、 Apple では 2 ステップ確認と呼ばれる同様のセキュリティ機能も提供しています。 2 ステップ確認を有効にした場合は、 Apple ID アカウント情報の変更を許可したり、 iCloud、 iMessage、 FaceTime、 Game Center にサインインしたり、 新しいデバイスで iTunes Store、 Apple Books、 Apple Store で買い物をしたりする前に、 ユーザの信頼できるいずれかのデバイスに送信される一時的なコードを使ってユーザの識別情報を確認する必要があります。 また、 ユーザには 14 文字の復旧キーが発行されます。 この復旧キーは安全な場所に保管しておき、 パスワードを忘れたり、 信頼できるデバイスにアクセスできなくなったりした場合に使用します。 ほとんどの新規ユーザに 2 ファクタ認証の使用が推奨されますが、 その代わりに 2 ステップ確認が推奨される状況もあります。

Apple ID の 2 ステップ確認について詳しくは、 次の Web サイトを参照してください。
support.apple.com/HT204152

管理対象 Apple ID

管理対象 Apple ID は、 通常の Apple ID と同じように機能しますが、 教育機関によって所有および管理されます。 教育機関は、 パスワードのリセット、 購入の制限、「FaceTime」や「メッセージ」などの通信の制限、 および教職員、 教師、 生徒のための役割に基づくアクセス権の設定などを実行できます。

管理対象 Apple ID では、 Apple Pay、 iCloud キーチェーン、 HomeKit、「iPhone を探す」など、 一部の Apple サービスを利用することができません。

管理対象 Apple ID について詳しくは、 次の Web サイトを参照してください。
help.apple.com/schoolmanager/#/tes78b477c81

管理対象 Apple ID の監査

管理対象 Apple ID は、 教育機関が法的規制やプライバシー規制を順守するための監査機能もサポートしています。 管理者、 マネージャ、 教師のアカウントなど、 特定の管理対象 Apple ID に監査権限を付与できます。 監査担当者が監視できるアカウントは、 学校の組織構成で自分より下位の階層にあるアカウントのみです。 つまり、 教師は生徒を監視できます。 また、 マネージャは教師と生徒を、 管理者はマネージャと教師と生徒を監査できます。

Apple School Manager を使用して資格情報の監査が要求されると、 監査が要求された管理対象 Apple ID のみにアクセスできる特別なアカウントが発行されます。 監査用アカウントは 7 日後に無効になります。 監査期間中、 監査担当者は、 iCloud または CloudKit 対応 App に保存されているユーザのコンテンツを表示および変更できます。 監査用のアクセス要求はすべて Apple School Manager のログに記録されます。 このログには、 監査担当者、 その担当者がアクセスを要求した管理対象 Apple ID、 要求日時、 監査の実行の有無が表示されます。

管理対象 Apple ID の監査について詳しくは、 次の Web サイトを参照してください。
help.apple.com/schoolmanager/#/tesd8fcbdd99

管理対象 Apple ID と個人用デバイス

管理対象 Apple ID を、 個人所有の iOS デバイスおよび Mac コンピュータで使用することもできます。 生徒が iCloud にサインインするには、 教育機関が発行した管理対象 Apple ID のほかに、 Apple ID の 2 ファクタ認証プロセスの第 2 要素として機能するパスワードを自分で作成します。 管理対象 Apple ID を個人所有デバイスで使用する場合は、 iCloud キーチェーンを使用できません。 また、「FaceTime」や「メッセージ」など、 ほかの機能が教育機関によって制限されることがあります。 生徒がサインイン中に作成した iCloud の書類はすべて、 このセクションで前述した監査の対象になります。

iMessage

Apple の iMessage は、iOS デバイス、Apple Watch、Mac コンピュータのメッセージサービスです。 iMessage では、 テキストに加え、 写真、 連絡先、 位置情報などを添付することも可能です。 メッセージは、 ユーザが登録したすべてのデバイスに表示されるので、 どのデバイスからも会話を続けることができます。 iMessage では Apple プッシュ通知サービス（APNs）が多く使用されます。 メッセージの内容や添付ファイルは Apple 側では記録されず、 エンドツーエンドの暗号化で保護されるため、送信者と受信者以外はだれもアクセスできません。 Apple がそのデータを復号することもできません。

ユーザがデバイスで iMessage をオンにすると、 そのサービスで使用される 2 つの鍵ペアが生成されます。 暗号化用の鍵（RSA 1280 ビット）と、署名用の鍵（NIST P-256 楕円曲線の ECDSA 256 ビット）です。 両方の鍵ペアの秘密鍵はデバイスのキーチェーンに保存されます。 公開鍵は Apple Identity Service（IDS）に送信され、 そこでユーザの電話番号またはメールアドレス、 およびデバイスの APNs アドレスに関連付けられます。

ユーザが iMessage で使用する追加のデバイスを有効にすると、 デバイスの暗号化および署名用公開鍵、 APNs アドレス、 および関連付けられた電話番号がディレクトリサービスに追加されます。 ユーザはメールアドレスを追加することもできます。 追加したアドレスは確認用リンクの送信によって確認されます。 電話番号は、 通信事業者のネットワークおよび SIM によって確認されます。 一部のネットワークでは、 そのために SMS を使用する必要があります（SMS が無料でない場合は、確認ダイアログが表示されます）。 iMessage のほかにも、 FaceTime や iCloud などのいくつかのシステムサービスで、電話番号の確認が必要な場合があります。 新しいデバイス、電話番号、またはメールアドレスが追加されると、 ユーザが登録したすべてのデバイスに通知メッセージが表示されます。

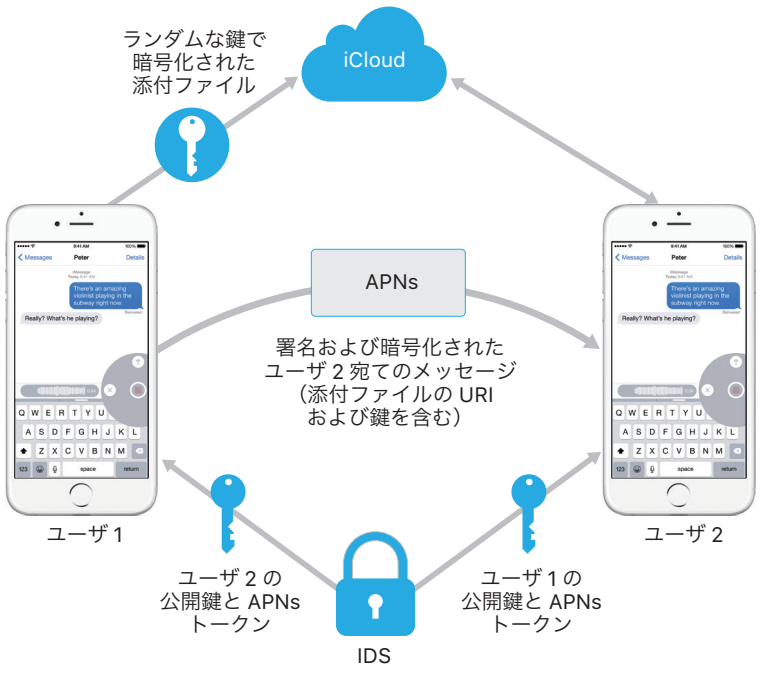
iOS 12 以降では、 同じ Apple ID にリンクされた異なるアドレスからのメッセージが、 受信側デバイスで 1 つの会話として表示されます。 これは、 アカウント識別子を、 メールアドレスまたは電話番号に対応する公開鍵および APNs アドレスと共に IDS から取得することによって実現されます。

iMessage のメッセージの送受信方法

iMessage で会話を開始するには、 相手のアドレスまたは名前を入力します。 ユーザが電話番号またはメールアドレスを入力すると、 デバイスは IDS と通信し、 受信者に関連付けられたすべてのデバイスの公開鍵と APNs アドレスを取得します。 ユーザが名前を入力すると、デバイスはまずユーザの「連絡先」を使用してその名前に関連付けられた電話番号およびメールアドレスを収集した後、IDS から公開鍵と APNs アドレスを取得します。

ユーザの送信メッセージは、 受信者のデバイスごとに個別に暗号化されます。 受信デバイスの公開 RSA 暗号鍵は、 IDS から取得されます。 送信デバイスは受信デバイスごとにランダムな 88 ビット値を生成し、 この値を HMAC-SHA256 鍵として使い、 送信者と受信者の公開鍵とプレーンテキストから導出される 40 ビット値を構成します。 88 ビット値と 40 ビット値を連結させて 128 ビット鍵を作り、この鍵を利用して AES の CTR モードでメッセージを暗号化します。40 ビット値は、 復号されたプレーンテキストの完全性を検証するために受信側で使用されます。 このメッセージごとの AES 鍵は、 RSA-OAEP を使用して受信デバイスの公開鍵に対して暗号化されます。 次に、 暗号化されたメッセージテキストと暗号化されたメッセージ鍵の組み合わせが SHA-1 を使ってハッシュ化され、 送信デバイスの署名用秘密鍵を用いてハッシュに ECDSA の署名が付加されます。 その結果、メッセージは、暗号化されたメッセージテキスト、暗号化されたメッセージ鍵、および送信者のデジタル署名から構成され、 受信デバイスごとに異なるメッセージになります。 この後メッセージは APNs に送られて配信されます。 タイムスタンプや APNs の経路情報などのメタデータは暗号化されません。 APNs との通信は、 前方秘匿性を持つ TLS チャネルを使用して暗号化されます。

APNs が中継できるメッセージのサイズは、iOS のバージョンにより最大 4KB または 16KB です。 メッセージのテキストが長すぎる場合、または写真などの添付ファイルが含まれる場合は、添付ファイルが、ランダムに生成された 256 ビット鍵で AES の CTR モードを用いて暗号化され、iCloud にアップロードされます。 次に、添付ファイルの AES 鍵、**URI（Uniform Resource Identifier）**、および暗号化結果の SHA-1 ハッシュが、iMessage の内容として受信者に送信されます。 それらの機密性と完全性は、次の図に示す標準の iMessage 暗号化機能によって保護されます。



グループ会話の場合は、各受信者のデバイスごとにこのプロセスが繰り返されます。

受信側では、各デバイスが APNs からメッセージのコピーを受信し、必要に応じて iCloud から添付ファイルを取得します。 可能な場合は名前を表示できるように、送信者の発信電話番号またはメールアドレスが受信者の連絡先と照合されます。

すべてのプッシュ通知と同様に、メッセージは配信された時点で APNs から削除されます。 ただし、ほかの APNs 通知と異なり、iMessage のメッセージはオフラインデバイスへの配信のためにキューに入れられます。 メッセージは現在、最長 30 日間保存されます。

ビジネスチャット

ビジネスチャットは、個人ユーザが「メッセージ」App で企業や店舗と会話できるようにするためのメッセージングサービスです。 会話を開始できるのはユーザのみで、企業や店舗はユーザを表す不特定の識別子を受け取ります。 ユーザの電話番号、メールアドレス、または iCloud アカウント情報が企業や店舗に送られることはありません。 Apple と会話するときは、Apple ID に関連付けられたビジネスチャット ID が Apple に送られます。 この場合も、会話をするかどうかの決定権はユーザにあります。 ビジネスチャットの会話を削除すると、ユーザの「メッセージ」App からその会話が削除され、以降、相手の企業・店舗はユーザにメッセージを送信できなくなります。

企業や店舗に送信されるメッセージはそれぞれ、ユーザのデバイスと Apple のメッセージングサーバ間で暗号化され、Apple のメッセージングサーバで復号されて、TLS 経由で企業や店舗に転送されます。 企業や店舗からの返信も同様に TLS 経由で Apple のメッセージングサーバに送信され、そこで暗号化されてユーザのデバイスに転送されます。 iMessage と同様に、オフラインデバイスに配信するため、メッセージは最長 30 日間キューに保存されます。

FaceTime

FaceTime は、 Apple のビデオおよびオーディオ通話サービスです。 iMessage と同様に、 FaceTime 通話では、 ユーザが登録したデバイスへの最初の接続を確立するために Apple プッシュ通知サービス（APNs）を使用します。 FaceTime 通話のオーディオ／ビデオコンテンツはエンドツーエンドの暗号化によって保護されるため、 送信者と受信者以外はだれもアクセスできません。 Apple がそのデータを復号することもできません。

FaceTime での最初の接続は、 ユーザが登録したデバイス間でデータパケットをリレーする Apple のサーバインフラストラクチャを介して行われます。 デバイスはリレー接続上で APNs 通知および STUN（Session Traversal Utilities for NAT）メッセージを使用して識別情報の証明書を確認し、 各セッションの共有シークレットを確立します。 共有シークレットは、 SRTP（Secure Real-time Transport Protocol）経由でストリーミングされるメディアチャネル用のセッション鍵の導出に使用されます。 SRTP パケットは Counter Mode の AES-256 と HMAC-SHA1 を使用して暗号化されます。 最初の接続とセキュリティの設定が行われた後の FaceTime では、 可能な場合は STUN および ICE（Internet Connectivity Establishment）を使用してデバイス間のピアツーピア接続を確立します。

グループ FaceTime を使うと、 最大 33 人の参加者が同時に FaceTime 通話を行うことができます。 従来の 1 対 1 の FaceTime と同様、 通話は招待された参加者のデバイス間でエンドツーエンドの暗号化によって保護されます。 1 対 1 の FaceTime のインフラストラクチャおよび設計のかなりの部分がそのまま使用されていますが、 グループ FaceTime 通話には、 IDS による真正性に加えて、 新しい鍵確立メカニズムが搭載されています。 このプロトコルにより前方秘匿性が提供されます。 つまり、 ユーザのデバイスが不正使用されても、 過去の通話の内容は漏洩しません。 セッション鍵は AES-SIV でラップされ、 P-256 ECDH の一時鍵による ECIES 構成を使用して参加者間で配付されます。

進行中のグループ FaceTime 通話に新しい電話番号やメールアドレスが追加されると、 有効なデバイスで新しいメディア鍵が確立され、 これまでに使用された鍵が新しく招待されたデバイスと共有されることはありません。

iCloud

iCloud にユーザの連絡先、 カレンダー、 写真、 書類などを保存すると、 ユーザのすべてのデバイスでこれらの情報を自動的に最新の状態に維持できます。 他社製 App も iCloud を使って、 書類や、 デベロッパによって定義された App データのキー値の保存および同期を行えます。 ユーザは Apple ID でサインインし、 使用したいサービスを選択して iCloud を設定します。「マイフォトストリーム」、 iCloud Drive、 iCloud バックアップなどの iCloud の機能は、 IT 管理者が MDM 構成プロファイルを使って無効にすることができます。 このサービスでは保存されるデータの種類は認識されず、 すべてのファイルコンテンツがバイトの集合体として同様に扱われます。

iCloud によって各ファイルがチャンクに分割され、 AES-128 と各チャンクのコンテンツから導出される、 SHA-256 を使用する鍵を使って暗号化されます。 それらの鍵とファイルのメタデータは Apple によってユーザの iCloud アカウントに保存されます。暗号化されたファイルのチャンクは、 Apple と他社の両方のストレージサービスに保存されます。 これらのチャンクには、 ユーザを特定する情報や鍵は含まれません。

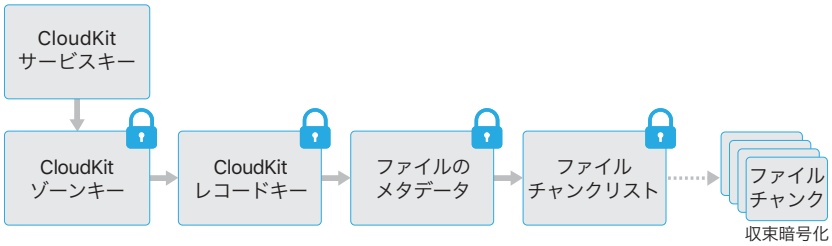
iCloud Drive

iCloud Drive では、 iCloud に保存されている書類を保護するためにアカウントに基づく鍵が追加されます。 既存の iCloud サービスと同様、 ファイルコンテンツがチャンクに分割されて暗号化され、 他社のサービスを利用して保存されます。 ただし、 ファイル・コンテンツ・キーは、 iCloud Drive のメタデータと一緒に保存されるレコードキーでラップされます。 これらのレコードキーも、 ユーザの iCloud Drive サービスキーによって保護されます。 この iCloud Drive サービスキーは、 ユーザの iCloud アカウントで保存されます。 ユーザは iCloud への認証によって iCloud 書類のメタデータにアクセスできますが、 iCloud Drive ストレージの保護されている部分を表示するには、 iCloud Drive サービスキーを所有している必要があります。

CloudKit

App デベロッパは CloudKit を使うことで、キー値データ、構造化データ、および各種アセットを iCloud に保存できます。CloudKit へのアクセスは App のエンタイトルメントを使用して制御されます。CloudKit は、公開データベースと非公開データベースの両方に対応しています。公開データベースは App のすべてのコピーで使用され、通常は一般的なアセット用であり、暗号化されません。非公開データベースにはユーザのデータが格納されます。

CloudKit は iCloud Drive と同様に、アカウントに基づく鍵を使用して、ユーザの非公開データベースに格納されている情報を保護します。また、ほかの iCloud サービスと同様に、ファイルはチャンクに分割されて暗号化され、他社のサービスを利用して保存されます。CloudKit ではデータ保護と同様の鍵階層を利用します。Per File キーは CloudKit レコードキーでラップされます。これらのレコードキーもゾーン鍵で保護され、ゾーンキーはユーザの CloudKit サービスキーで保護されます。CloudKit サービスキーはユーザの iCloud アカウントに保存され、ユーザが iCloud で認証を完了してはじめて利用可能になります。



CloudKit のエンドツーエンドの暗号化

Apple Pay Cash、ヘルスケアデータ、ユーザキーワード、Siri、Hey Siri では、iCloud キーチェーンの同期で保護された CloudKit サービスキーにより提供される、CloudKit のエンドツーエンドの暗号化が使用されます。これらの CloudKit コンテナでは、鍵階層のルートが iCloud キーチェーンにあるため、iCloud キーチェーンのセキュリティ特性が共有されます。鍵は信頼できるデバイスでのみ使用でき、Apple も他社も使用できません。iCloud キーチェーンのデータへのアクセスが失われると（後述の「エスクローのセキュリティ」セクションを参照）、CloudKit のデータがリセットされます。信頼できるローカルデバイスでそれらのデータが使用可能な場合は、CloudKit に再アップロードされます。

「iCloud にメッセージを保管」機能でも、iCloud キーチェーンの同期で保護された CloudKit サービスキーにより提供される、CloudKit のエンドツーエンドの暗号化が使用されます。ユーザが iCloud バックアップを有効にした場合は、「iCloud にメッセージを保管」コンテナで使用される CloudKit サービスキーが iCloud にバックアップされます。これにより、ユーザは、iCloud キーチェーンや信頼できるデバイスにアクセスできなくなった場合でも、メッセージを復元できます。この iCloud サービスキーは、ユーザが iCloud バックアップを無効にするとローリングされます。

iCloud バックアップ

iCloud では、デバイス設定、App データ、「カメラロール」の写真やビデオ、「メッセージ」App でのやりとりといった情報を Wi-Fi 経由で毎日バックアップすることもできます。iCloud はコンテンツをインターネット経由で送信する際に暗号化し、暗号化フォーマットで保存します。さらに、認証にセキュアトークンを使うことでコンテンツを確実に保護します。iCloud バックアップは、デバイスがロックされて電源に接続され、かつ Wi-Fi 経由でインターネットに接続できる場合にのみ実行されます。iOS が使用する暗号化により、データを安全に保護しながら、差分の無人バックアップと復元を実行することができます。

復元オプション

状況	CloudKit のエンドツーエンドの暗号化でのユーザ復元オプション
信頼できるデバイスを利用可能	信頼できるデバイスまたは iCloud キーチェーン復元によるデータ復元が可能
信頼できるデバイスなし	iCloud キーチェーン復元によるデータ復元のみ可能

状況	「iCloud にメッセージを保管」でのユーザ復元オプション
iCloud バックアップが有効で、信頼できるデバイスを利用可能	iCloud バックアップ、信頼できるデバイス、または iCloud キーチェーン復元によるデータ復元が可能
iCloud バックアップが有効で、信頼できるデバイスなし	iCloud バックアップまたは iCloud キーチェーン復元によるデータ復元が可能
iCloud バックアップが無効で、信頼できるデバイスを利用可能	信頼できるデバイスまたは iCloud キーチェーン復元によるデータ復元が可能
iCloud バックアップが無効で、信頼できるデバイスなし	iCloud キーチェーン復元によるデータ復元のみ可能

iCloud では以下の項目のバックアップが作成されます。

- 購入した音楽、映画、テレビ番組、App、およびブックについてのレコード。 ユーザの iCloud バックアップにはユーザの iOS デバイスに表示される購入したコンテンツについての情報が含まれますが、購入したコンテンツ自体は含まれません。 ユーザが iCloud バックアップから復元すると、購入したコンテンツが iTunes Store、 Apple Books、 または App Store から自動的にダウンロードされます。 一部の種類のコンテンツが自動的にダウンロードされない国または地域もあります。 また、 コンテンツが払い戻された場合や、 ストアで扱われなくなった場合、 以前に購入したコンテンツを利用できなくなることがあります。 全購入履歴はユーザの Apple ID に関連付けられています。
- ユーザの iOS デバイス上の写真とビデオ。 ユーザが iOS デバイス（iOS 8.1 以降）または Mac（OS X 10.10.3 以降）の iCloud フォトライブラリをオンにしている場合、 写真とビデオはすでに iCloud に保存されているため、 ユーザの iCloud バックアップには含まれません。
- 連絡先、 カレンダーイベント、 リマインダー、 メモ
- デバイス設定
- App データ
- 通話履歴と着信音
- ホーム画面および App の配置
- HomeKit の構成
- Visual Voicemail のパスワード （バックアップ時に使用した SIM カードが必要）
- iMessage、ビジネスチャット、 テキスト （SMS）、および MMS メッセージ （バックアップ時に使用した SIM カードが必要）

注意：「iCloud にメッセージを保管」 を有効にした場合は、 iMessage、ビジネスチャット、テキスト （SMS）、および MMS メッセージがユーザの既存の iCloud バックアップから削除され、代わりに、エンドツーエンドで暗号化されたメッセージ用 CloudKit コンテナに保存されます。 ユーザの iCloud バックアップには、 そのコンテナへの鍵が保持されます。 その後、 ユーザが iCloud バックアップを無効にすると、 そのコンテナの鍵がローリングされ、 新しい鍵が iCloud キーチェーンにのみ保存されて （Apple も他社もアクセスできません）、 コンテナに書き込まれた新しいデータは古いコンテナの鍵では復号できなくなります。

デバイスのロック中にアクセスできないデータ保護クラスでファイルが作成されると、 Per File キーは iCloud バックアップキーバッグにあるクラスキーを使用して暗号化されます。 ファイルは元の暗号化された状態で iCloud にバックアップされます。 データ保護クラス No Protection のファイルは、 転送中に暗号化されます。

iCloud バックアップキーバッグには、 各データ保護クラス用の非対称 （Curve25519） 鍵が含まれます。 これらは Per File キーの暗号化に使用されます。 バックアップキーバッグおよび iCloud バックアップキーバッグの内容について詳しくは、 この文書の 「暗号化とデータ保護」 セクションの 「キーチェーンのデータ保護」 を参照してください。

バックアップセットはユーザの iCloud アカウントに保存されます。 これは、 ユーザのファイルのコピーと、 iCloud バックアップキーバッグで構成されます。 iCloud バックアップキーバッグはランダムな鍵によって保護されます。 この鍵もバックアップセットと一緒に保存されます。 （ユーザの iCloud パスワードは暗号化に使用されないため、 iCloud パスワードを変更しても既存のバックアップが無効になることはありません。）

ユーザのキーチェーンデータベースは iCloud にバックアップされますが、 UID と関連付けられた鍵によって常に保護されます。 そのため、 キーチェーンはバックアップの作成元と同じデバイスにのみ復元できます。 つまり、 Apple を含む他者がユーザのキーチェーン項目を読み出すことはできません。

復元時には、 バックアップされたファイル、 iCloud バックアップキーバッグ、 およびキーバッグ用の鍵が、ユーザの iCloud アカウントから取得されます。iCloud バックアップキーバッグがキーバック用の鍵で復号された後、 キーバッグにある Per File キーを使ってバックアップセット内のファイルが復号されます。 それらのファイルは新しいファイルとしてファイルシステムに書き込まれるため、それぞれのデータ保護クラスに従って再暗号化されます。

iCloud キーチェーン

Safari と iCloud キーチェーンの統合
「Safari」では、 Web サイトのパスワード用に、暗号の仕組みを用いた強力でランダムな文字列を自動的に作成できます。 この文字列はキーチェーンに保存され、 ほかのデバイスと同期されます。 キーチェーン項目は Apple のサーバを経由してデバイス間で転送されますが、 Apple もほかのデバイスも内容を読み出せないように暗号化されます。

iCloud キーチェーンを使うと、 Apple に情報を開示することなく、 iOS デバイスや Mac コンピュータの間でパスワードを安全に同期することができます。 強力なプライバシーと安全性に加え、iCloud キーチェーンの設計とアーキテクチャにおいて重視されているのは、 使いやすさとキーチェーンの復元性です。 iCloud キーチェーンは、 キーチェーン同期とキーチェーン復元という 2 つのサービスで構成されます。

Apple は、 ユーザのパスワードが以下のような状況でも保護されるように iCloud キーチェーンとキーチェーン復元を設計しています。

- ユーザの iCloud アカウントが不正使用された。
- 外部の攻撃者または従業員によって iCloud が不正使用された。
- ユーザアカウントに第三者がアクセスした。

キーチェーン同期

ユーザが iCloud キーチェーンをはじめて有効にすると、 デバイスが信頼グループを確立し、 そのデバイス自体の同期識別情報を作成します。 同期識別情報は秘密鍵と公開鍵で構成されます。 同期識別情報の公開鍵は信頼グループの中に置かれ、 そのグループは 2 回署名されます。 まず同期識別情報の秘密鍵で署名され、 次にユーザの iCloud アカウントパスワードから導出される楕円曲線の非対称鍵 （P-256 を使用）で署名されます。 信頼グループと共に、 ユーザの iCloud パスワードに基づく鍵の作成に使用されるパラメータ （ランダムなソルトおよび反復回数） も保存されます。

署名された同期グループはユーザの iCloud のキー値ストレージ領域に配置されます。 この読み出しにはユーザの iCloud パスワードが必要であり、グループメンバーの同期識別情報の秘密鍵がないと正規に変更を加えられません。

ユーザが別のデバイス上で iCloud キーチェーンをオンにすると、 そのデバイスがメンバーになっていない iCloud 同期グループをユーザがすでに確立していることを、 そのデバイスが認識します。新しいデバイスはその同期識別情報の鍵ペアを作成してから、 グループのメンバーシップを要求する申請チケットを作成します。 このチケットはデバイスの同期識別情報の公開鍵で構成され、 ユーザは iCloud パスワードでの認証を求められます。 楕円曲線暗号鍵の生成パラメータが iCloud から取得され、これによって申請チケットの署名に使用される鍵が生成されます。最後に、申請チケットが iCloud に配置されます。

申請チケットの受信が最初のデバイスに認識されると、 新しいデバイスによる同期グループへの参加要求を承認するようユーザに求める通知が最初のデバイスに表示されます。 ユーザが iCloud パスワードを入力すると、 一致する秘密鍵で署名された申請チケットであることが確認されます。これによって、 グループへの参加要求を行った本人が、 その要求時にユーザの iCloud パスワードを入力したことが確認されます。

新しいデバイスをグループに追加することをユーザが承認すると、最初のデバイスが新しいメンバーの公開鍵を同期グループに追加し、自らの同期識別情報と、ユーザの iCloud パスワードから導出された鍵の両方を使って再度公開鍵に署名します。新しい同期グループが iCloud に配置されます。その同期グループには、グループの新しいメンバーも同様に署名しています。

これで同期グループのメンバーが 2 つになり、各メンバーがお互いの公開鍵を持つことになります。メンバー同士で iCloud のキー値ストレージを経由して個別のキーチェーン項目のやりとりが開始されるか、キーチェーン項目が適宜 CloudKit に保存されます。両方のグループメンバーに同じ項目がある場合、変更日が最も新しい項目が同期されます。他方のメンバーに同じ項目があり、変更日も同一の場合はスキップされます。同期される各項目は暗号化され、ユーザの信頼グループに含まれるデバイスによってのみ復号できるようになります。ほかのデバイスや Apple が復号することはできません。

新しいデバイスが同期グループに追加されると、このプロセスが繰り返されます。たとえば、デバイスがもう 1 つ参加した場合、ユーザの残りのデバイスの両方に確認メッセージが表示されます。ユーザはそのどちらかのデバイスで新しいメンバーを承認できます。新しいメンバーが追加されると、各メンバーが新しいメンバーと同期され、すべてのメンバーのキーチェーン項目が同じ内容になります。

ただし、キーチェーン全体は同期されません。VPN ID などの一部の項目はデバイス固有のものであり、そのデバイス以外には送信されません。属性が `kSecAttrSynchronizable` の項目のみが同期されます。Apple は、Safari ユーザデータ（ユーザ名、パスワード、およびクレジットカード番号を含む）と、Wi-Fi パスワードおよび HomeKit の暗号鍵にこの属性を設定しています。

また、デフォルトでは、他社製 App によって追加されたキーチェーン項目は同期されません。デベロッパは、キーチェーンに項目を追加する際に `kSecAttrSynchronizable` を設定する必要があります。

キーチェーン復元

キーチェーン復元では、ユーザは Apple がパスワードおよびその他のデータを読み取れるようにすることなく、必要に応じてキーチェーンを Apple にエスクロー（預託）することができます。ユーザは、デバイスを 1 つしか持っていない場合でも、キーチェーン復元によってデータの損失を防止できます。これは、Safari を使って Web のアカウント用にランダムで強力なパスワードを生成する場合に特に重要です。これらのパスワードの記録はキーチェーンにしか残らないためです。

キーチェーン復元は、この機能をサポートするために Apple が開発した二次認証と安全なエスクローサービスによって実現されます。ユーザのキーチェーンは強力なパスコードを使って暗号化され、条件が厳密に満たされた場合にのみ、エスクローサービスからキーチェーンのコピーが提供されます。

iCloud キーチェーンをオンにしたとき、そのユーザのアカウントで 2 ファクタ認証が有効になっていれば、エスクローしたキーチェーンがデバイスのパスコードを使って復元されます。2 ファクタ認証が設定されていない場合、ユーザは 6 桁のパスコードを指定して iCloud セキュリティコードを作成するよう求められます。または、2 ファクタ認証を使用せずに、ユーザが独自の長いコードを指定したり、暗号の仕組みによるランダムなコードをデバイスに作成させて、それを自分で記録して保管したりすることもできます。

次に、iOS デバイスがユーザのキーチェーンのコピーを書き出し、非対称キーバッグにある鍵でラップして暗号化し、ユーザの iCloud のキー値ストレージ領域に保存します。キーバッグはユーザの iCloud セキュリティコードと、エスクローレコードが保存される HSM（ハードウェア・セキュリティ・モジュール）クラスタの公開鍵でラップされます。これがユーザの iCloud エスクローレコードになります。

ユーザが、独自のセキュリティコードを指定したり、4 桁の値を使用したりするのではなく、暗号の仕組みによるランダムなセキュリティコードを生成して使用することを決定した場合は、エスクローレコードは不要です。その代わりに、iCloud セキュリティコードを使用してランダムな鍵が直接ラップされます。

ユーザはセキュリティコードを設定するだけでなく、電話番号も登録する必要があります。これにより、キーチェーン復元で別の段階での認証を行うことができます。ユーザには SMS が送信され、復元を進めるにはこの SMS に返信する必要があります。

エスクローのセキュリティ

iCloud には、認証されたユーザおよびデバイスのみが復元を実行できるようにするためのキーチェーンエスクロー向けに安全なインフラストラクチャが用意されています。iCloud を背後で支えているのが、エスクローレコードを保護する HSM クラスタです。クラスタごとに鍵があり、この文書で前述したように、その鍵を使ってクラスタの監視下でエスクローレコードを暗号化します。

キーチェーンを復元するには、ユーザが iCloud アカウントとパスワードで認証し、登録済みの電話番号に送信される SMS に返信する必要があります。その後、ユーザは iCloud セキュリティコードを入力する必要があります。HSM クラスタは SRP（Secure Remote Password）プロトコルを使用して、ユーザが iCloud セキュリティコードを知っていることを確認します。コード自体は Apple に送信されません。クラスタの各メンバーは、ユーザがレコードを取得する際に許容される最大試行回数（後述）を超えていないことをそれぞれで確認します。超えていないという判断で過半数が一致した場合は、エスクローレコードがアンラップされ、レコードがユーザのデバイスに送信されます。

次に、デバイスが iCloud セキュリティコードを使用して、ユーザのキーチェーンの暗号化に使用したランダムな鍵をアンラップします。その鍵を使って、iCloud のキー値ストレージから取得されたキーチェーンが復号され、デバイス上に復元されます。認証およびエスクローレコード取得の試行は、最大 10 回のみ許容されます。試行に数回失敗するとレコードがロックされるため、それ以上試行するには、ユーザは Apple サポートに電話して承認を得る必要があります。10 回失敗すると、HSM クラスタによってエスクローレコードが破棄され、キーチェーンが完全に失われます。これは、キーチェーンデータを犠牲にする代わりに、レコードの取得を試みる総当たり（ブルートフォース）攻撃からレコードを守る手段になります。

これらのポリシーは HSM ファームウェアに組み込まれています。ファームウェアの変更を許可する管理アクセスカードは破棄されています。ファームウェアの改ざんまたは秘密鍵へのアクセスが試行されると、HSM クラスタによって秘密鍵が削除されます。万一この状況が発生した場合は、そのクラスタによって保護されている各キーチェーンの所有者に、エスクローレコードが失われたことを通知するメッセージが送信されます。それらのユーザは、その後再登録ができます。

Siri

自然に話しかけるだけで、Siri はメッセージを送信したり、会議のスケジュールを設定したり、電話をかけたりしてくれます。Siri は、音声認識、テキスト読み上げ、クライアントサーバモデルを使ってさまざまなリクエストに答えます。Siri がサポートするタスクは、ごく最小限の個人情報のみが完全に保護された状態で利用されるように設計されています。

Siri をオンにすると、音声認識および Siri サーバで使用されるランダムな識別子が作成されます。これらの識別子は、サービスの向上のため Siri の内部でのみ使用されます。その後 Siri をオフにすると、再度 Siri をオンにしたときに使用されるランダムな識別子が新しく生成されます。

Siri の機能を向上させるため、ユーザの情報の一部がデバイスからサーバに送信されます。これには、ミュージックライブラリについての情報（曲のタイトル、アーティスト、プレイリスト）、「リマインダー」のリスト名、「連絡先」で定義されている名前と続柄などが含まれます。サーバとの通信はすべて HTTPS で行われます。

Siri セッションが開始されると、「連絡先」から取得されたユーザの名と姓が、大まかな位置情報と共にサーバに送信されます。これによって、Siri が応答に名前を含めたり、天気に関する質問など大まかな位置情報のみが必要な質問に答えたりできます。

付近の映画館の場所を調べるときのように、位置を正確に特定する必要がある場合は、より正確な位置情報を送信するようにサーバがデバイスに要求します。これは、デフォルトではユーザのリクエストを処理するために本当に必要な場合にのみ情報がサーバに送信されるということを示す一例です。どのような場合でも、使用しない状態が 10 分間続くと、セッション情報が破棄されます。

Apple Watch から Siri にリクエストした場合、 Apple Watch は、 上で述べたように、 独自のランダムな一意の識別子を作成します。 ただし、 ユーザの情報を再度送信するのではなく、 ペアリングされた iPhone の Siri 識別子を送信して、 その情報との関係性を示します。

ユーザが話した言葉の録音が Apple の音声認識サーバに送信されます。 タスクの内容が音声入力のみの場合は、 認識されたテキストがデバイスに送信されます。 その他の場合は、 Siri がテキストを分析し、 必要に応じて、 デバイスに関連付けられたプロフィールの情報と組み合わせます。 たとえば、「お母さんにメッセージを送信して」というリクエストの場合は、「連絡先」から取得された続柄と名前が使用されます。 その後、 認識されたアクションのコマンドが、 デバイスに返送されて実行されます。

Siri の機能の多くは、サーバの指示の下でデバイスによって実行されます。 たとえば、受信したメッセージを読むことをユーザが Siri に依頼した場合、 サーバは未開封のメッセージの内容を読み上げるようにデバイスに指示します。 メッセージの内容と送信者はサーバに送信されません。

ユーザの音声の録音は、 認識システムがユーザの音声認識の精度を高める目的で利用できるように 6 か月間保存されます。 6 か月経過した後は、 Apple が Siri の改善および開発のために使用できるように、識別子を削除した別のコピーが最長 2 年間保存されます。 録音、トランスクリプト、関連データの中で、 識別子を含まないごく一部のデータは、 Siri の継続的な改善と品質保証のために 2 年経過後も使用される場合があります。 また、 音楽、スポーツチームや選手、 企業、店舗や特定の場所に関する音声録音の一部も、 Siri を改善する目的で同様に保存されます。

Siri は音声コマンドによりハンズフリーで呼び出すこともできます。 音声トリガーの検出は、 デバイス上でローカルに行われます。 このモードでは、 入力された音声パターンが、 指定されたトリガーフレーズの音響に十分一致した場合にのみ Siri が起動します。 トリガーが検出されると、 その後に入力された Siri コマンドを含むオーディオが Apple の音声認識サーバに送信されます。 ここからは、 Siri で行われるユーザのその他の音声録音と同じルールにそって処理されます。

Apple Watch では、 ユーザが手首を上げて、 Apple Watch を口元に近付けて Siri に話しかけることで Siri を呼び出すこともできます。 Siri は、 次の両方の条件が満たされたときに起動します。

- デバイス上の機械学習モデルによって、 デバイス付近で人間の声が検出される
- デバイス上の 2 つ目の機械学習モデルによって、「手首を上げて話す」 ジェスチャーと一致するモーションプロファイルとデバイスのポーズが検出される

このオーディオとモーションの組み合わせが検出されると、 対応するオーディオが Apple の音声認識サーバに送信されます。 ここからは、 Siri で行われるユーザのその他の音声録音と同じルールにそって処理されます。

Siri からの提案

Siri からの App やショートカットの提案は、デバイス上の機械学習を用いて生成されます。 ショートカットや App の起動のきっかけとなる状況を予測する上でどの情報が有用だったかについて、ユーザを特定できない一部のデータが Apple に送信される場合はありますが、 それ以外のデータが送信されることはありません。

Siri のショートカット

Siri に追加されたショートカットは、 iCloud を利用するすべての Apple デバイス間で同期され、CloudKit のエンドツーエンドの暗号処理により暗号化されます。 ショートカットに関連付けられたフレーズは、 音声認識のため Siri サーバに同期され、ランダムな Siri 識別子に関連付けられます（「Siri」 セクションを参照）。 ショートカットの内容は Apple に送信されず、 ローカルのデータストアに保存されます。

「ショートカット」 App

「ショートカット」 App のカスタムショートカットは、 iCloud を使用して Apple デバイス間で同期するように選択できます。 iCloud 経由でほかのユーザとショートカットを共有することもできます。

カスタムショートカットは、スクリプトやプログラムと同じように幅広い用途に使用できます。 インターネットからダウンロードされたショートカットは、 検疫システムによって隔離されます。 ユーザがそのショートカットをはじめて使用するときは警告が表示され、ショートカットに関する情報（提供元など）を確認できます。

「Safari」で共有シートからカスタムショートカットを呼び出して、 Web サイト上でユーザ指定の JavaScript を実行することもできます。 この際、 ユーザを巧みに誘導し、 SNS サイトでスクリプトを実行させてデータを盗み取ったりする悪質な JavaScript からユーザを守るため、 実行時に、 悪質なスクリプトを検出するための最新のマルウェア定義がダウンロードされます。 ユーザがドメイン上ではじめて JavaScript を実行するときは、 そのドメインの現在の Web ページで JavaScript を含むショートカットの実行を許可するかどうかの確認が求められます。

Safari 検索候補、 Siri からの提案、「調べる」、 # イメージ、「News」 App、 および 「News」 が提供されていない国での「News」 ウィジェット

Safari 検索候補、Siri からの提案、「調べる」、# イメージ、「News」 App、および 「News」 が提供されていない国での「News」 ウィジェットには、 Wikipedia、 iTunes Store、 ローカルニュース、「マップ」 の検索結果、 App Store など、 デバイス外のソースから取得された、 検索候補や提案が表示されます。これらはユーザが入力を開始する前から表示されることもあります。

ユーザが「Safari」のアドレスバーで入力を開始したり、Siri からの提案を使用したり、「調べる」を使用したり、 # イメージを開いたり、「News」 App で検索を使用したり、「News」 が提供されていない国での「News」 ウィジェットを使用したりすると、 以下のコンテキストが HTTPS で暗号化されて Apple に送信され、 該当する結果がユーザに提供されます。

- プライバシーを保護するために 15 分おきに入れ替えられる識別子。
- ユーザの検索クエリ。
- コンテキストおよびローカルにキャッシュされた過去の検索に基づく、 最も可能性の高いクエリ補完。
- デバイスの大まかな位置 （「位置情報サービス」 で 「位置情報に基づく検索候補」 がオンになっている場合)。 位置情報を 「大まかにする」 度合いは、 デバイスの現在位置の推定人口密度に基づきます。 たとえば、 ユーザ同士が地理的に大きく離れている可能性がある地方ではより大まかになり、 一般にユーザが密集する都市の中心部ではあまり大まかになりません。 ユーザは「設定」 の 「位置情報サービス」 で 「位置情報に基づく検索候補」 をオフにすることで、 Apple へのあらゆる位置情報の送信を無効にできます。 位置情報サービスがオフになっている場合でも、 Apple はデバイスの IP アドレスを使用しておおよその位置を推測することがあります。
- デバイスの種類と検索が実行されている機能 （Siri からの提案、「Safari」、「調べる」、「News」 App、 または 「メッセージ」)。
- 接続の種類。
- デバイス上で最後に使用された 3 つの App の情報 （補足的な検索コンテキストを知るため)。 Apple が管理する一般的な App の許可リストに含まれ、 かつ過去 3 時間以内にアクセスされた App のみが含まれます。
- デバイス上で使用頻度が高いアプリケーションのリスト。
- 地域の言語、 ロケール、 および入力環境設定。
- ユーザのデバイスが音楽やビデオのサブスクリプションサービスに登録している場合、 サブスクリプションサービスの名前やサブスクリプションの種類などの情報が Apple に送信される場合があります。 ユーザのアカウント名、 番号、 およびパスワードは Apple に送信されません。
- 関心のあるトピックを集約し要約したデータ。

ユーザがいずれかの検索結果を選択するか、結果を選択せずに App を終了すると、将来の検索結果の品質向上に役立てるため、一部の情報が Apple に送信されます。この情報は同じ 15 分間のセッション識別子にのみ関連付けられ、特定のユーザには関連付けられません。このフィードバックには、上記のコンテキスト情報の一部に加え、以下のような操作に関する情報も含まれます。

- 操作と検索ネットワーク要求間のタイミング。
- 検索候補や提案のランキングと表示順序。
- 検索結果の ID と選択されたアクション（結果が位置情報に基づかない場合）、または選択された結果のカテゴリ（位置情報に基づく場合）。
- ユーザが結果を選択したかどうかを示すフラグ。

Apple は検索候補や提案のログを、クエリ、コンテキスト、およびフィードバックと共に 18 か月間保持します。ログの一部は最大 5 年間保持されます（クエリ、ロケール、ドメイン、大まかな位置情報、集約されたメトリクスなど）。

場合によっては、検索候補や提案で、認定パートナーの検索結果を受信して表示するために、一般的な単語や語句のクエリが認定パートナーに転送されることがあります。Apple は、パートナーがクエリと共にユーザの IP アドレスや検索フィードバックを受信しないように、プロキシを介してクエリを送信します。パートナーとの通信は HTTPS で暗号化されます。Apple は頻繁に実行されるクエリについて、検索パフォーマンスを改善するために、都市レベルの位置情報、デバイスの種類、クライアントの言語を検索コンテキストとしてパートナーに送信します。

さまざまな地理的位置およびネットワークの種類における検索候補や提案のパフォーマンスを把握して改善するため、以下の情報がセッション識別子を使わずに記録されます。

- 部分的な IP アドレス（IPv4 アドレスの場合は末尾の 8 ビット、IPv6 アドレスの場合は末尾の 80 ビットを抜いたもの）
- 大まかな位置情報
- クエリの大まかな時刻
- レイテンシ／転送速度
- 応答のサイズ
- 接続の種類
- ロケール
- デバイスの種類とリクエスト元の App

Safari の賢い追跡防止機能

「Safari」には、Cookie および Web サイトデータに関する、プライバシーに配慮したデフォルトポリシーの一部として、賢い追跡防止機能（ITP）が搭載されています。Cookie およびその他の Web サイトデータへのアクセスを制限することにより、サイト越えトラッキングを防ぎます。

ITP では、リソース負荷（イメージやスクリプトなど）の統計とユーザ操作（タップやテキスト入力など）の情報が収集されます。収集された統計を基に、機械学習モデルによって、どのドメイン名がサイトを超えてユーザを追跡できるかが、デバイス上で分類されます。

追跡能力を持つドメインとして分類されると、ユーザが以前にそのドメインをファーストパーティとして利用し、何らかの操作を行ったことがある場合は、その Cookie がただちに分離されます。また、ユーザがそのドメインで操作を行ったことがない場合は、その Cookie がただちにブロックされます。たとえば以下のような動作になります。

- video.example は、広告が表示されないサブスクリプションサービスを提供しており、その動画の多くはほかの Web サイトに埋め込まれている
- ユーザが video.example にサインインしてから、video.example のコンテンツが埋め込まれたほかの Web サイトにアクセスする

- ITP は video.example を追跡能力を持つドメインとして分類し、その Cookie を分離する
- ユーザが newspaper.example にアクセスし、そこに video.example の動画が埋め込まれていた場合、video.example に渡される Cookie は、newspaper.example 上の video.example に固有の分離済み Cookie になる

埋め込まれたサードパーティコンテンツが、Storage Access API を介して自ドメインのファーストパーティ Cookie にアクセスすることを求める場合があります。「Safari」で、Storage Access API を使用する埋め込みサードパーティコンテンツをユーザがタップまたはクリックすると、サードパーティにその Cookie および Web サイトデータへのアクセスを許可するかどうかを尋ねるメッセージが表示されます。許可すると、サードパーティはファーストパーティドメインでユーザを追跡できるようになります。ユーザが「許可」を選択した場合、埋め込みサードパーティコンテンツは、そのページが表示されている間、自ドメインのファーストパーティ Cookie にアクセスすることを許可されます。以降、ユーザがそのページにアクセスし、埋め込みサードパーティコンテンツを操作すると、コンテンツによって Storage Access API が呼び出され、そのファーストパーティ Cookie にアクセスできるようになります。このアクセスはユーザが以前に許可しているので、許可を求めるメッセージは表示されません。ユーザの選択は、ファーストパーティとサードパーティの組み合わせに対して保持され、ユーザが「Safari」の閲覧履歴を消去すると選択は取り消されます。

追跡能力を持つと分類されたドメインの既存の Cookie は、ユーザが「Safari」を使用してそのドメインで 30 日間何も操作（直接的な操作または Storage Access API を介した操作）を行わなかった場合に消去されます。30 日間操作が行われないと、追跡能力を持つと分類されたドメインは新しい Cookie をセットすることもできなくなります。「Safari」では、サードパーティのコンテキストでほかのファーストパーティの Web サイトデータにアクセスすることは禁止されています。

ITP によりファーストパーティとサードパーティデータを分離することで、サイト越えトラッキングを目的とする Cookie および Web サイトデータの使用を防止できます。特定のデバイスが統計を収集したドメイン名や追跡能力を持つと分類されたドメイン名が Apple に伝えられることはありません。

ITP では、追跡能力を持つと分類されたドメインに対して、サードパーティ Cookie がブロックされるだけでなく、送信される HTTP リファラー情報もそのページの参照元のみに制限されます。

ユーザパスワード管理

iOS には、パスワード認証を使用する他社製の App や Web サイトでユーザが安全かつ便利に認証を行えるようにするための、さまざまな機能が用意されています。パスワードは、特殊なパスワード自動入力キーチェーンに保存されます。このキーチェーンは、「設定」>「パスワードとアカウント」>「Web サイトと App のパスワード」でユーザが管理できます。App は、ユーザの許可なくパスワード自動入力キーチェーンにアクセスすることはできません。iCloud キーチェーンを有効にした場合は、パスワード自動入力キーチェーンに保存された資格情報がデバイス間で同期されます。

iCloud キーチェーンのパスワードマネージャとパスワード自動入力では、以下の機能を利用できます。

- App や Web サイトで資格情報を入力する
- 強力なパスワードを作成する
- App と「Safari」の Web サイトの両方のパスワードを保存する
- 連絡先に登録されている人とパスワードを安全に共有する
- 資格情報の入力を求める近くの Apple TV にパスワードを送信する

保存済みパスワードへのアクセス

共有 Web 証明書 API

iOS App では、次の 2 つの API を使ってパスワード自動入力キーチェーンを操作できます。

`SecRequestSharedWebCredential`

`SecAddSharedWebCredential`

App のデベロッパと Web サイトの管理者の承認およびユーザの同意がある場合にのみ、iOS App にアクセスが許可されます。App のデベロッパは App にエンタイトルメントを含めることで、「Safari」に保存されたパスワードにアクセスする意思を表明できます。このエンタイトルメントには、関連する Web サイトの完全修飾ドメイン名のリストが記載されます。Web サイトは、Apple が承認した App の一意の App 識別子のリストを記載したファイルをサーバに配置する必要があります。

com.apple.developer.associated-domains エンタイトルメントを持つ App がインストールされると、iOS がリスト内の各 Web サイトに TLS リクエストを発行し、次のいずれかのファイルを要求します。

- apple-app-site-association
- .well-known/apple-app-site-association

インストールされる App の App 識別子がファイルのリストにある場合は、その Web サイトと App が信頼関係にあるとマークされます。信頼関係がある場合にのみ、これら 2 つの API を呼び出したときにユーザにプロンプトが表示されます。ユーザがこれに同意しない限り、パスワードを App に渡したり、アップデートまたは削除したりすることはできません。

App のパスワードの自動入力

iOS では、キーボードの QuickType バーに表示される「鍵」の機能をタップすることで、App の認証関連フィールドに、保存済みのユーザ名とパスワードを入力できます。このときも同様に、App と Web サイトを強固に関連付けるために、apple-app-site-association ファイルを使った関連付けの仕組みが利用されます。このインターフェイスでは、ユーザが資格情報を App に渡すことを承諾するまで、資格情報は App に提供されません。iOS によって Web サイトと App 間の信頼関係が認識されると、その App での資格情報の入力時に、QuickType バーで適切な入力候補が直接表示されます。これにより、App に API が実装されていない場合でも、ユーザは同じセキュリティ特性を利用して、「Safari」に保存された資格情報を App に提供できるようになります。

App と Web サイト間に信頼関係がある場合、ユーザが App 内から資格情報を送信すると、それらの資格情報を次回以降利用できるようにパスワード自動入力キーチェーンに保存するかどうかを確認するメッセージが表示されることがあります。

強力なパスワードの自動作成

iCloud キーチェーンを有効にすると、ユーザが App 内または「Safari」の Web サイト上でユーザ登録を行うときやパスワードを変更するときに、iOS によって強力な一意のパスワードがランダムに作成されます。強力なパスワードの作成機能はデフォルトで有効になります。作成されたパスワードはキーチェーンに保存され、iCloud キーチェーンを有効にしたデバイス間で同期されます。

iOS によって作成されるパスワードの長さは、デフォルトで 20 文字です。このパスワードには、1 桁の数字、1 文字の大文字、2 つのハイフン、16 文字の小文字が含まれます。このように作成される文字列は、エントロピーが 71 ビットの強力なパスワードになります。

App や「Safari」でパスワードが自動作成されるかどうかは、パスワードフィールドがパスワード作成用であるかどうかを判断するヒューリスティックに基づいて決まります。ヒューリスティックでパスワードコンテキストがパスワード作成用であると認識されない場合、デベロッパは、App の場合はテキストフィールドに UITextContentType.newPassword、Web サイトの場合は <input> 要素に autocomplete="new-password" を設定できます。

App や Web サイトは、作成されるパスワードが該当サービスの要件を満たせるように、iOS にパスワード規則を提供できます。iOS では、その規則に基づく最も強力なパスワードが作成されます。この規則を提供するには、UITextInputPasswordRules を使用するか、<input> 要素で passwordrules 属性を使用します。

ほかの人またはデバイスへのパスワード送信

AirDrop

iCloud を有効にすると、ユーザは保存済みの資格情報（対象 Web サイト、ユーザ名、パスワードなど）をほかのデバイスに AirDrop で送信できます。AirDrop による資格情報の送信は、ユーザの設定に関係なく常に「連絡先のみ」モードで行われます（詳しくは「AirDrop のセキュリティ」を参照）。受信側のデバイスでユーザが同意すると、そのユーザのパスワード自動入力キーチェーンに資格情報が保存されます。

Apple TV

Apple TV の App で資格情報を入力するときにパスワードの自動入力を利用できます。tvOS でユーザがユーザ名またはパスワードのテキストフィールドを選択すると、Apple TV が Bluetooth Low Energy（BLE）によるパスワード自動入力要求のアドバタイズメントを開始します。

近くにある iPhone には、 Apple TV が資格情報の共有を求めていることを知らせるメッセージが表示されます。 iPhone と Apple TV が同じ iCloud アカウントを使用している場合は、このプロセスの間、 デバイス間の通信が暗号化されます。 iPhone が Apple TV とは異なる iCloud アカウントにサインインしている場合は、 以下の操作が必要です。

- PIN コードを使用して暗号化接続を確立する
- メッセージを受信するために iPhone のロックを解除し、 Apple TV とペアリングされた Siri Remote に iPhone を近付ける

Bluetooth LE リンクの暗号化を使用して暗号化通信が確立されると、 資格情報が Apple TV に送信され、 App の該当テキストフィールドに自動入力されます。

クレデンシャルプロバイダ機能拡張

ユーザは、「パスワードとアカウント」 設定で、 対応する他社製 App を AutoFill クレデンシャルプロバイダ （自動入力の資格情報提供者）として指定できます。 これは機能拡張を利用したメカニズムです。 クレデンシャルプロバイダ機能拡張では、 資格情報を選択するためのビューを提供する必要があります。 オプションで、 QuickType バーで入力候補を直接表示するために、 保存済み資格情報に関する iOS メタデータを提供することもできます。 このメタデータには、 資格情報の対象 Web サイトと、 関連付けられたユーザ名が含まれますが、 パスワードは含まれません。 パスワードは、 ユーザが App または「Safari」 の Web サイトで入力するときに、 iOS が機能拡張と通信して取得します。 資格情報のメタデータは、 クレデンシャルプロバイダのサンドボックス内に保存され、 App のアンインストール時に自動的に削除されます。

デバイスの管理

iOS は、 適用および管理しやすい柔軟なセキュリティポリシーと構成をサポートしています。 これにより、 BYOD プログラムの一環として社員が自ら用意したデバイスを使用する場合でも、 組織は企業情報を保護し、 社員に企業の要件を順守するよう徹底することが可能です。

組織は、 パスコード保護、 構成プロファイル、 リモートワイプ、 他社製 MDM ソリューションといったリソースを活用して多数のデバイスを管理し、 社員が個人所有の iOS デバイスで企業データにアクセスする場合でもそのデータを保護することができます。

パスコードによる保護

デフォルトでは、 ユーザのパスコードは数字の PIN として定義できます。 Touch ID または Face ID を搭載するデバイスの場合、 最も短いパスコードは 4 桁です。 ユーザが「設定」 > 「パスコード」 の「パスコードオプション」 で「カスタムの英数字コード」 を選択すると、 より長い英数字のパスコードを指定できます。 推測や攻撃を困難にするために、 長く複雑なパスコードが推奨されます。

管理者は MDM または Exchange ActiveSync を使用して、 あるいは構成プロファイルを手動でインストールするようユーザに求めることで、 複雑なパスコードの要件を適用できます。 以下のパスコードポリシーを適用できます。

- 単純値を許可
- 英数字の値が必要
- 最短のパスコード
- 複合文字の最小数
- パスコードの最長の有効期限
- パスコードの履歴
- 自動ロックのタイムアウト
- デバイスロックの猶予期間
- 入力を失敗できる回数
- Touch ID または Face ID を許可

各ポリシーの管理者向けの詳細は、 次の Web サイトを参照してください。
help.apple.com/deployment/mdm/#/mdm4D6A472A

各ポリシーのデベロッパ向けの詳細は、 次の Web サイト（英語） を参照してください。
developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef

iOS のペアリングモデル

iOS では、 ペアリングモデルを使ってホストコンピュータからデバイスへのアクセスを制御します。 ペアリングにより、 デバイスとそれに接続されたホストとの間に信頼関係が確立されます。 この際、 公開鍵の交換が信頼の証となります。 iOS では、 この信頼の証を使用することで、 接続されたホストとの間でデータ同期などの追加機能を実現します。

iOS 9 では、ペアリングが必要なサービスはユーザがデバイスのロックを解除するまで起動できません。

また、 iOS 10 以降では、 写真の同期などの一部のサービスを開始するためにデバイスのロックを解除する必要があります。

iOS 11 以降では、 デバイスのロックを最近解除していない限りサービスは起動しません。

ペアリングプロセスでは、 ユーザがデバイスのロックを解除し、 ホストからのペアリング要求を受け入れる必要があります。 iOS 11 以降では、 ユーザがパスコードを入力する必要もあります。 ユーザがこれらの操作を行うと、 ホストとデバイスが 2048 ビットの RSA 公開鍵を交換して保存します。 次に、 デバイス上に保存されているエスクローキーバッグのロックを解除できる 256 ビットの鍵がホストに提供されます (この文書の「キーバッグ」セクションの「エスクローキーバッグ」を参照)。 交換された鍵を使って、暗号化された SSL セッションを開始します。 デバイスから保護されたデータをホストに送信したり、 サービス （iTunes 同期、 ファイル転送、 Xcode 開発など） を開始したりするには、 事前にこのセッションを開始する必要があります。 デバイスでこの暗号化されたセッションをすべての通信に使用するには、 ホストから Wi-Fi 経由で接続する必要があるため、 デバイスをあらかじめ USB でペアリングしておく必要があります。 ペアリングによって、 いくつかの診断機能も有効になります。 iOS 9 では、 ペアリングの記録は 6 か月以上使用されないと期限切れになります。 iOS 11 以降ではさらに短縮され、 30 日で期限切れになります。

詳しくは、 次の Web サイトを参照してください。
support.apple.com/kb/HT6331

com.apple.pcapd などの特定のサービスは、 USB 経由でのみ機能するように制限されています。 また、 com.apple.file_relay サービスでは、 Apple が署名した構成プロファイルをインストールする必要があります。

iOS 11 以降では、 Secure Remote Password プロトコルを使用して Apple TV とのペアリングをワイヤレスで確立できます。

ユーザは 「ネットワーク設定をリセット」 または 「位置情報とプライバシーをリセット」 オプションを使用して、 信頼できるホストのリストを消去できます。

詳しくは、 次の Web サイトを参照してください。
support.apple.com/kb/HT5868

構成の適用

構成プロファイルは、 管理者が構成情報を iOS デバイスに配付するために使用できる XML ファイルです。 インストールされた構成プロファイルで定義されている設定をユーザが変更することはできません。 ユーザが構成プロファイルを削除すると、 そのプロファイルで定義されたすべての設定も削除されます。 管理者はこの方法で、 ポリシーを Wi-Fi やデータアクセスに関連付けることで、 ポリシーの設定を徹底することができます。 たとえば、 メールの設定を行うための構成プロファイルで、 デバイスのパスコードポリシーを指定することもできます。 その場合、 ユーザは管理者が定めた要件を満たすパスコードを使用しない限り、 メールにアクセスできません。

iOS 構成プロファイルには、 次のような多数の設定項目があります。

- パスコードポリシー
- デバイスの機能制限 （カメラを無効にするなど）
- Wi-Fi 設定
- VPN 設定
- メールサーバ設定
- Exchange 設定
- LDAP ディレクトリサービスの設定
- CalDAV カレンダーサービスの設定
- Web クリップ
- 資格情報とその鍵
- モバイルデータ通信ネットワークの詳細設定

管理者向けの最新リストについては、 次の Web サイトを参照してください。
help.apple.com/deployment/mdm/#/mdm5370d089

デベロッパ向けの最新リストについては、次の Web サイト（英語）を参照してください。
developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef

構成プロファイルは、署名と暗号化を行うことで、提供元の検証や、完全性の確保、コンテンツの保護を行うことができます。構成プロファイルは、3DES および AES-128 をサポートする CMS（RFC 3852）を使用して暗号化されます。

また、構成プロファイルをデバイスにロックして、削除を完全に防止したり、パスワードを入力した場合のみ削除可能にしたりすることもできます。多くの企業のユーザが個人所有の iOS デバイスを使用しているため、デバイスを MDM ソリューションにバインドする構成プロファイルは削除できます。ただし、削除すると、管理対象の構成情報、データ、および App もすべて削除されます。

ユーザは Apple Configurator 2 を使って構成プロファイルをデバイスに直接インストールできます。また、構成プロファイルを「Safari」でダウンロードしたり、メールで受信したり、MDM ソリューションを使用してワイヤレスで受信したりすることもできます。ユーザが Apple School Manager または Apple Business Manager でデバイスを設定した場合は、MDM 登録用のプロファイルがデバイスによってダウンロードおよびインストールされます。

モバイルデバイス管理（MDM）

iOS は MDM に対応しているため、企業は、大規模に導入されている iPhone、iPad、Apple TV、Mac を安全に設定し、管理することができます。MDM の機能は、構成プロファイル、ワイヤレスでの登録、Apple プッシュ通知サービス（APNs）などの既存の iOS テクノロジーを基礎としています。たとえば、APNs は、デバイスが MDM ソリューションとセキュリティ保護された接続で直接通信できるようにデバイスをスリープ解除する目的で使用されます。機密情報や専有情報が APNs 経由で送信されることはありません。

IT 部門は MDM を使用することで、企業環境への iOS デバイスの登録、ワイヤレスでの設定の構成や更新、企業ポリシーへの準拠状況の監視、ソフトウェア・アップデート・ポリシーの管理、管理対象デバイスのリモートワイプやリモートロックなどを行うことができます。

MDM について詳しくは、次の Web サイトを参照してください。

- www.apple.com/iphone/business/it/management.html
- help.apple.com/deployment/ios/#/ior07301dd60
- help.apple.com/deployment/mdm/#/mdmbf9e668

共有 iPad

共有 iPad とは、iPad を導入した教育機関が使用するマルチユーザモード構成の iPad のことです。複数の生徒が書類やデータを共有することなく 1 台の iPad を共有できます。生徒にはそれぞれ、APFS ボリュームとして作成されユーザの資格情報で保護された個別のホームディレクトリが割り当てられます。共有 iPad では、学校が発行および所有する管理対象 Apple ID を使用する必要があります。共有 iPad は複数の生徒で使用できるように構成されているため、生徒は教育機関が所有するどの iPad にもサインインできます。生徒のデータは、それぞれのデータ保護ドメイン内の個別のホームディレクトリに分割され、各ディレクトリは UNIX のアクセス権とサンドボックスの両方で保護されます。

共有 iPad にサインインする

生徒がサインインすると、管理対象 Apple ID が Apple の認証サーバによって SRP プロトコル経由で認証されます。認証に成功すると、そのデバイス専用の一時的なアクセストークンが付与されます。生徒がそのデバイスを以前に使ったことがある場合は、同じ資格情報を使用してロック解除されたローカルユーザアカウントがすでに設定されています。

生徒がそのデバイスを以前に使ったことがない場合は、新しい UNIX ユーザ ID、APFS ボリュームとユーザのホームディレクトリ、およびキーチェーンがプロビジョニングされます。そのデバイスがインターネットに接続していない場合は（校外学習中など）、特定の期間のみローカルアカウントを

使用して認証できます。 この場合は、 既存のローカルアカウントを持っているユーザのみがサインインできます。 所定の期間が過ぎると、 ローカルアカウントを持っていてもオンラインでの認証を求められます。

生徒のローカルアカウントがロック解除または作成され、 リモートで認証されると、 Apple のサーバによって発行された一時的なトークンが、 iCloud へのサインインを許可する iCloud トークンに変換されます。 次に、 生徒の設定が復元され、 その生徒の書類やデータが iCloud から同期されます。

生徒のセッションが進行中でデバイスがオンラインになっている間は、 書類やデータが作成または変更されると iCloud に保存されます。 また、 バックグラウンドで同期する仕組みによって、 生徒のサインアウト後も変更内容が iCloud にプッシュされます。 ユーザのバックグラウンド同期が完了すると、 そのユーザの APFS ボリュームがマウント解除され、 そのユーザの資格情報を入力するまで再度マウントできなくなります。

共有 iPad からサインアウトする

生徒が共有 iPad からサインアウトすると、 生徒のユーザキーバッグがただちにロックされ、 すべての App が終了されます。 このとき、 次に使う生徒がすばやくサインインできるように、 通常のサインアウト処理の一部が一時保留になり、 新しい生徒にログインウインドウが表示されます。 この保留時間 （約 30 秒） 内に生徒がサインインした場合は、 新しい生徒のアカウントのサインイン過程で、 保留されたクリーンアップが実行されます。 共有 iPad がアイドル状態のままの場合は、 保留されたクリーンアップが開始されます。 クリーンアップ段階では、 別のサインアウトが発生したかのようにログインウインドウが再開されます。

共有 iPad のアップグレード

共有 iPad を iOS 10.3 より前のバージョンから iOS 10.3 以降にアップグレードすると、 1 回限りのファイルシステム変換が実行され、 HFS+ データパーティションが APFS ボリュームに変換されます。 その時点でシステム上にユーザのホームディレクトリが存在する場合、 それらは個々の APFS ボリュームに変換されず、 メインデータボリューム上に残ります。

その後に新しい生徒がサインインすると、 その生徒のホームディレクトリもメインデータボリューム上に置かれます。 メインデータボリューム上のすべてのユーザアカウントが削除されるまで、 前述のように新規ユーザアカウントで個別の APFS ボリュームが作成されることはありません。 そのため、 APFS による追加の保護と割り当て容量をユーザに提供するには、 iPad を iOS 10.3 以降にアップグレードする際にクリーンインストールを選択するか、 MDM のユーザ削除コマンドを使用してデバイス上のすべてのユーザアカウントを削除する必要があります。

共有 iPad について詳しくは、 次の Web サイトを参照してください：
help.apple.com/deployment/mdm/#/cad7e2e0cf56

Apple School Manager

Apple School Manager は、 教育機関がコンテンツの購入、 MDM ソリューションでの自動デバイス登録の設定、 生徒と教職員用アカウントの作成、 iTunes U コースの設定などを行えるサービスです。 Apple School Manager はテクノロジー担当者、 IT 管理者、 教職員、 教師を対象として設計されており、 Web からアクセスできます。

Apple School Manager について詳しくは、 次の Web サイトを参照してください。
help.apple.com/schoolmanager

Apple Business Manager

Apple Business Manager は、 IT 管理者が iOS、 macOS、 および tvOS デバイスを 1 か所からまとめて導入できる、 シンプルな Web ベースのポータルです。 モバイルデバイス管理 （MDM） ソリューションと組み合わせることで、 デバイスを設定したり、 App やブックを購入して配付したりできます。 Apple Business Manager は IT 管理者を対象として設計されており、 Web からアクセスできます。

Apple Business Manager について詳しくは、次の Web サイトを参照してください：
help.apple.com/businessmanager

デバイス登録

Apple School Manager と Apple Business Manager では、組織が Apple または Apple 正規取扱店か通信事業者から直接購入した iOS デバイスを、すばやく効率的に導入できます。iOS 11 以降または tvOS 10.2 以降を搭載したデバイスの場合は、購入後に Apple Configurator 2 を使用して Apple School Manager や Apple Business Manager に追加することもできます。

組織はユーザに渡す前に、デバイスに触れたり準備したりすることなく、デバイスを MDM に自動的に登録できます。いずれかのプログラムに登録した後、管理者はプログラムの Web サイトにサインインし、プログラムを MDM ソリューションにリンクさせます。その後、購入したデバイスを MDM 経由でユーザに割り当てることができるようになります。デバイスの設定プロセス中に、次のようなセキュリティ対策を適切に実施することで、機密データのセキュリティを強化できます。たとえば以下のようになります。

- Apple デバイスのアクティベーション時に、設定アシスタントの初期設定手順の一部としてユーザによる認証を強制する。
- アクセスが制限される暫定的な設定を用意し、機密データへのアクセスには追加のデバイス設定を求める。

ユーザの割り当てが完了すると、MDM で指定された構成、制限、または制御が自動的にインストールされます。デバイスと Apple サーバ間のすべての通信は、HTTPS（SSL）経由で転送時に暗号化されます。

iOS、tvOS、および macOS の設定アシスタントで特定の手順を省略してユーザの設定プロセスをさらに簡素化できるため、ユーザがすぐにデバイスを使い始めることができます。管理者は、ユーザがデバイスから MDM プロファイルを削除できるかどうかを制御することも、はじめからデバイスに制限を設定しておくこともできます。デバイスを箱から出してアクティベートすると、デバイスが組織の MDM ソリューションに登録され、すべての管理設定、App、およびブックがインストールされます。

Apple Configurator 2

MDM だけでなく macOS 用の Apple Configurator 2 でも、ユーザに渡す前に iOS デバイスや Apple TV の設定と事前構成を簡単に行えます。Apple Configurator 2 を使用すると、デバイスに App、データ、機能制限、および設定をすばやく事前構成できます。

Apple Configurator 2 では、Apple School Manager または Apple Business Manager を使用して MDM ソリューションに登録できるため、ユーザが設定アシスタントを使う必要はありません。また、iOS デバイスや Apple TV の購入後に Apple Configurator 2 を使用して Apple School Manager または Apple Business Manager に追加することもできます。

Apple Configurator 2 について詳しくは、次の Web サイトを参照してください。
help.apple.com/configurator/mac

監視モード

デバイスの設定中に、デバイスを監視対象として構成することができます。監視対象であるということは、デバイスが組織に所有されているということです。そのため、デバイスの構成および制限がより厳密に制御されます。Apple School Manager または Apple Business Manager では、MDM 登録プロセスの一部としてワイヤレスで、または Apple Configurator 2 を使用して手動で、監視モードを有効にできます。デバイスを監視モードにするには、デバイスを消去して、再度アクティベーションする必要があります。

MDM または Apple Configurator 2 を使用した iOS デバイスおよび Apple TV の構成と管理について詳しくは、次の Web サイトを参照してください。
help.apple.com/deployment/ios

機能制限

管理者は、機能制限を有効にしたり、場合によっては無効にしたりすることで、特定の App、サービス、またはデバイスの機能をユーザが利用できないように制限することができます。機能制限は、構成プロファイルに添付される機能制限ペイロードとしてデバイスに送信されます。機能制限は iOS、tvOS、macOS デバイスに適用できます。管理対象の iPhone では、ペアリングされている Apple Watch にも特定の機能制限が反映されます。

IT マネージャ向けの最新リストについては、次の Web サイトを参照してください。
help.apple.com/deployment/mdm/#/mdm0F7DD3D8

リモートワイプ

iOS デバイスは、管理者またはユーザがリモートで消去できます。Effaceable Storage からブロックストレージの暗号鍵を安全に破棄し、すべてのデータを読み取れない状態にすることによって、リモートワイプを瞬時に実行できます。リモート・ワイプ・コマンドは、MDM、Exchange、または iCloud によって開始できます。

リモート・ワイプ・コマンドが MDM または iCloud によって発行されると、デバイスは確認応答を送信し、ワイプを実行します。Exchange によるリモートワイプの場合は、デバイスが Exchange サーバにチェックインしてから、ワイプを実行します。

ユーザも、自分が所有するデバイスを「設定」App でワイプできます。前に述べたように、パスコードの誤入力が続いた場合にデバイスが自動的にワイプされるように設定することもできます。

紛失モード

iOS 9.3 以降を搭載する監視モードのデバイスでは、紛失または盗難に遭った場合に、MDM 管理者がリモートで紛失モードを有効にできます。紛失モードが有効になると、現在のユーザはログアウトされ、デバイスのロックを解除できなくなります。画面には、デバイスを見つけた人が連絡するための電話番号など、管理者がカスタマイズできるメッセージが表示されます。デバイスが紛失モードになると、管理者はそのデバイスに対して現在の位置情報を送信するよう要求できます。オプションで、サウンドを再生するように指示することもできます。管理者が紛失モードをオフにすると（これが紛失モードを終了する唯一の方法です）、そのことがロック画面またはホーム画面のメッセージでユーザに通知されます。

アクティベーションロック

「iPhone を探す」がオンの場合、デバイスを再びアクティベーションするには所有者の Apple ID のアカウント情報またはデバイスの以前のパスコードを入力する必要があります。

組織が所有するデバイスでは、再アクティベーションのために各ユーザが自分の Apple ID アカウント情報を入力しなくても済むように、デバイスを監視モードに設定して組織がアクティベーションロックを管理できるようにすることをお勧めします。

監視モードのデバイスでは、対応する MDM ソリューションを使用して、アクティベーションロックが有効になった時点でバイパスコードを保存しておき、後でデバイスを消去して別のユーザに割り当てる必要が生じたときにはこのコードを使ってアクティベーションロックを自動的に解除することができます。

デフォルトでは、ユーザが「iPhone を探す」をオンにした場合でも、監視モードのデバイスのアクティベーションロックは有効になりません。ただし、MDM ソリューションがバイパスコードを取得し、デバイスでのアクティベーションロックの有効化を許可する場合があります。MDM

ソリューションがデバイスのアクティベーションロックを有効にしたときに「iPhone を探す」がオンになっていると、その時点でアクティベーションロックが有効になります。MDM サーバがアクティベーションロックを有効にしたときに「iPhone を探す」がオフになっていると、アクティベーションロックはユーザが次回「iPhone を探す」をオンにしたときに有効になります。

Apple School Manager で作成された管理対象 Apple ID を使う教育機関用のデバイスでは、アクティベーションロックをユーザの Apple ID ではなく管理者の Apple ID に関連付けたり、デバイスのバイパスコードを使用して無効にしたりすることができます。

スクリーンタイム

スクリーンタイムは iOS 12 から搭載された機能で、ユーザ自身または子供のデバイスの App や Web の使用状況を把握して管理することができます。スクリーンタイムでは以下のことが可能です。

- 使用状況を表示する
- App や Web の使用制限を設定する
- 休止時間を設定する
- その他の制限を適用する

自身のデバイスの使用状況を管理する場合は、同じ iCloud アカウントを使用するデバイス間で CloudKit のエンドツーエンドの暗号化を使用して、スクリーンタイムのコントロールと使用状況データを同期できます。そのためには、ユーザのアカウントで 2 ファクタ認証を有効にする必要があります（同期はデフォルトではオフです）。スクリーンタイムは、iOS の以前のバージョンに搭載されていた制限機能に代わるものです。

ユーザが「Safari」の履歴を消去したり App を削除したりすると、該当する使用状況データが、そのデバイスおよび同期するすべてのデバイスから削除されます。

保護者とスクリーンタイム

保護者は iOS デバイスでスクリーンタイムを使用して、子供のデバイス使用状況を把握して管理することもできます。保護者が iCloud ファミリー共有の管理者である場合は、子供の使用状況データを表示し、スクリーンタイム設定を管理することができます。保護者がスクリーンタイムをオンにすると、子供に通知され、子供も自身の使用状況を監視できるようになります。保護者は、子供のスクリーンタイムをオンにするときに、子供が設定を変更できないようにパスコードを設定することができます。子供は、18 歳になった日から（年齢は国や地域によって異なります）、この監視をオフにできます。

保護者のデバイスと子供のデバイス間では、使用状況データと設定が、Apple Identity Service（IDS）によるエンドツーエンドの暗号化接続を介して転送されます。暗号化されたデータは、受信側のデバイスで準備が整うまで IDS サーバに一時保存される場合があります（iPhone/iPad がオフであった場合はオンになるまでの間など）。このデータを Apple が読み取ることはできません。

スクリーンタイムの解析

ユーザが「iPhone と Watch 解析を共有」をオンにした場合は、Apple がスクリーンタイム機能の使用状況をより適切に理解できるように、次の匿名データのみが収集されます。

- スクリーンタイムをどこでオンにしたか（設定アシスタント、または初期設定後の「設定」）
- スクリーンタイムがオンかどうか
- 休止時間が有効かどうか
- 「時間延長の許可を求める」リクエストの使用回数
- App 制限数

App や Web の具体的な使用状況データが Apple によって収集されることはありません。スクリーンタイムの使用状況画面に表示される App リストのアイコンは、App Store から直接取得されます。取得時の要求に関するデータも一切保持されません。

プライバシーコントロール

Apple はお客様のプライバシーを重視しており、 App がユーザの情報を利用する方法と条件や、利用する情報の種類をユーザが決定できるように、 さまざまな仕組みやオプションを iOS に組み込んでいます。

位置情報サービス

位置情報サービスでは、 GPS、 Bluetooth、 クラウドソーシングの Wi-Fi ホットスポットや携帯基地局の位置を使って、 ユーザのおおよその位置を判断します。 位置情報サービスは、「設定」 にあるスイッチを 1 つ切り替えるだけでオフにできます。 または、 このサービスを利用する App ごとにアクセスを承認することもできます。 App の使用中のみ位置情報データの利用を許可することも、 常に許可することもできます。 このアクセスを許可しないと選択した場合も、「設定」 からいつでも変更できます。「設定」 では、 App が要求する位置情報の用途に応じて、 許可しない、 使用中のみ許可、 常に許可のいずれかに設定できます。 また、 位置情報を常に使用できるよう許可した App がバックグラウンドモードでこの許可を利用する場合は、 ユーザが許可したことが通知されるので、 必要に応じて App への許可を変更できます。

さらに、 システムサービスによる位置情報の利用も、 ユーザが細かく制御できます。 たとえば、 Apple が iOS を改善するために利用する解析サービスで収集される情報や、 位置情報に基づく Siri の情報、 Siri からの提案での位置情報に基づくコンテキスト、 周辺の交通情報、 過去利用頻度の高い場所といった情報に、 位置情報を含めないように設定できます。

個人データへのアクセス

iOS では、 App がユーザの個人情報に許可なくアクセスすることを防止できます。 また、「設定」では、 ユーザが特定の情報へのアクセスを許可した App を確認し、 今後アクセスすることを許可または取り消すことができます。 これには、 以下の項目へのアクセスが含まれます。

- 連絡先
- カレンダー
- リマインダー
- 写真
- モーションとフィットネス
- 位置情報サービス
- Apple Music
- 音楽やビデオの操作
- マイク
- カメラ
- HomeKit
- ヘルスケア
- 音声認識
- Bluetooth 共有
- メディアライブラリ

ユーザが iCloud にサインインしている場合は、 iCloud Drive へのアクセスがデフォルトで App に与えられます。 ユーザは「設定」 の「iCloud」 で各 App のアクセスを管理できます。 また、 iOS では、 MDM ソリューションによってインストールされた App およびアカウントと、 ユーザがインストールした App およびアカウントとの間で、 データ移動を禁止する制限を設定することもできます。

プライバシーポリシー

Apple のプライバシーポリシーについては、 次の Web サイトを参照してください。
www.apple.com/legal/privacy/jp

セキュリティに関する認定とプログラム

注意：iOS セキュリティに関する認定書、評価、ガイダンスの最新情報については、次の Web サイトを参照してください。
support.apple.com/kb/HT202739

ISO 27001/27018 認証

Apple は、2017 年 7 月 11 日付の適用宣言書（Statement of Applicability v2.1）により、製品およびサービス（Apple School Manager、iTunes U、iCloud、iMessage、FaceTime、管理対象 Apple ID、Siri、Schoolwork）をサポートするインフラストラクチャ、開発、運用管理について、情報セキュリティ・マネジメント・システムの ISO 27001 認証および ISO 27018 認証を取得しました。Apple が ISO 規格に準拠していることは、BSI（英国規格協会）によって認定されています。ISO 27001 および ISO 27018 準拠の認定書は、BSI の Web サイトに掲載されています。これらの認定書は、次の Web サイトで確認できます。

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

暗号認定（FIPS 140-2）

iOS の暗号モジュールは、iOS 6 以降、リリースするたびに米国連邦情報処理規格（FIPS）140-2 に準拠していることが認定されています。メジャーリリースごとに、Apple は iOS オペレーティングシステムのリリース時に再認定のために CMVP にモジュールを提出しています。このプログラムは、iOS の暗号化サービスと承認済みアルゴリズムを適切に使用する Apple の App および他社製 App の暗号演算の完全性を保証するプログラムです。

Apple は、**Apple Secure Enclave Processor（SEP）Secure Key Store（SKS）Cryptographic Module** として識別される組み込みハードウェアモジュールについて FIPS 140-2 認定を受け、SEP で生成および管理される鍵の使用を承認されました。Apple は、今後の iOS のメジャーリリースでも、必要に応じてハードウェアモジュールに関するより高度な認証の取得を目指します。

コモンクライテリア認証（ISO 15408）

iOS 9 のリリース以来、Apple は iOS のメジャーリリースごとに、コモンクライテリア認証プログラムの認証を取得し、その範囲を広げてきました。これまでに以下の認証を取得しています。

- Mobile Device Fundamental Protection Profile
  - Extended Package for Mobile Device Management Agents
  - Extended Package for Wireless LAN Clients
  - PP-Module for VPN Client
- Protection Profile for Application Software
  - Extended Package for Web Browsers

iOS 12 ではさらに以下の認証も取得できる見込みです。

- Extended Package for Email Clients

Apple は、 今後の iOS のメジャーリリースでも対象範囲を拡大していく予定です。

Apple は、International Technical Community（ITC）で、主要なモバイルセキュリティテクノロジーを評価する Collaborative Protection Profile（cPP）の開発で積極的な役割を果たしてきました。 Apple は今後も、 現在利用可能な cPP および開発中の cPP の新しいバージョンやアップデートされたバージョンの評価と、 それに基づいた認証を目指していきます。

Commercial Solutions for Classified（CSfC）

Apple は、 Commercial Solutions for Classified（CSfC）プログラムのコンポーネントリストへの追加のために、 適宜 iOS プラットフォームと各種サービスを提出しています。 Apple のプラットフォームとサービスは、 コモンクライテリア認証の審査を受ける過程で、 CSfC プログラムのコンポーネントリストへの追加を検討する対象としても提出されます。

最新のコンポーネントリストについては、 次の Web サイト（英語）を参照してください。
www.nsa.gov/resources/everyone/csfc/components-list

セキュリティ構成ガイド

Apple は世界各国の政府と協力し、 より安全な環境を維持する（ハイリスク環境での「デバイスハードニング」とも呼ばれる）ための手順や推奨事項を記載した各種ガイドを策定しています。 これらのガイドには、 保護を強化するための iOS の内蔵機能の設定および利用方法について、 十分に検証された具体的な情報が記載されています。

Apple セキュリティバウンティ

Apple は、 重大な問題について Apple に情報提供した研究者を対象に報奨金の支払いを行っています。 Apple セキュリティバウンティ（報奨金プログラム）の対象となるには、 明確な報告書と検証可能な概念実証（PoC）の提出が必要です。 対象となる脆弱性は、 最新リリースの iOS、および該当する場合は最新のハードウェアに影響するものに限られます。 実際の報奨金額は、 Apple によるレビュー後に決定されます。 この際、 発見の難しさ、 危険度、 必要なユーザ操作の度合いなどが基準になります。

問題の存在が確認された場合、 Apple は問題の早期解決を優先事項とします。 また、 適切な場合は、 情報提供者を表彰します（要請により辞退も可能）。

カテゴリ	最高支払額（米ドル）
セキュア・ブート・ファームウェア・コンポーネント	$200,000
Secure Enclave で保護されている機密資料の抽出	$100,000
カーネル権限による任意のコードの実行	$50,000
Apple サーバ上の iCloud アカウントデータへの不正アクセス	$50,000
サンドボックス化されたプロセスから、 そのサンドボックスの外部にあるユーザデータへのアクセス	$25,000

まとめ

セキュリティへの取り組み

Apple は、 個人情報を保護するために設計されたプライバシーおよびセキュリティに関する先進的な技術と、 企業環境内での企業データの保護に役立つ包括的な手法により、 お客様を守ることに力を注いでいます。

iOS にはセキュリティが組み込まれています。 プラットフォームからネットワーク、 さらには App まで、 企業に必要なあらゆるものが iOS プラットフォームで利用可能です。 iOS ではこれらの要素を組み合わせることで、 ユーザ体験を犠牲にすることなく、 業界をリードするセキュリティを実現しています。

Apple は、 iOS および iOS App のエコシステム全体を通じて、 一貫した統合セキュリティ基盤を採用しています。 ハードウェアベースのストレージ暗号化により、 デバイスを紛失した場合にリモートワイプ機能を使用でき、 デバイスを他者に売却または譲渡する場合にもユーザがすべての企業情報と個人情報を完全に削除できます。 診断情報も匿名で収集されます。

Apple が設計した iOS App は、 高度なセキュリティを念頭に置いて開発されています。 たとえば、 iMessage や FaceTime ではクライアント間の通信が暗号化されます。 他社製 App については、 必須のコード署名、 サンドボックス化、 およびエンタイトルメントを組み合わせることで、 ウイルス、 マルウェア、 その他の悪用に対する業界トップレベルの保護をユーザに提供します。 App Store の提出プロセスは、 すべての iOS App を公開前にレビューすることによって、 さらにユーザを保護する役割を果たします。

iOS に組み込まれた幅広いセキュリティ機能を最大限に活用するため、 企業には自社の IT ポリシーとセキュリティポリシーを見直し、 このプラットフォームで提供されている何重ものセキュリティを十分活かせるものにすることをお勧めします。

Apple には、 すべての Apple 製品を担当するセキュリティ専門チームがあります。 このチームは開発中の製品とリリース済みの製品の両方に対して、 セキュリティ監査とテストを実施しています。 また、 セキュリティツールやトレーニングを提供し、 セキュリティ上の新しい問題や脅威のレポートも積極的にモニタリングしています。 Apple は Forum of Incident Response and Security Teams（FIRST）にも参加しています。

Apple への問題の報告およびセキュリティ通知の購読について詳しくは、 次の Web サイトを参照してください。
www.apple.com/jp/support/security

用語集

アドレス空間配置のランダム化（ASLR）	iOS に採用されている、ソフトウェアのバグの悪用をはるかに困難にする技術。 メモリアドレスとオフセットが予測不能になるため、 悪意のあるコードでそれらの値をハードコーディングできなくなります。 iOS 5 以降では、 すべてのシステム App およびライブラリの位置がランダム化されると共に、 すべての他社製 App が位置に依存しない実行可能ファイルとしてコンパイルされます。
Apple Identity Service（IDS）	iMessage の公開鍵、APNs アドレス、および電話番号とメールアドレスを含む Apple のディレクトリ。 鍵およびデバイスのアドレスの検索に使用されます。
Apple Push Notification service（APNs）	iOS デバイスにプッシュ通知を配信する、 Apple が世界中で提供しているサービス。
ブート・プログレス・レジスタ（BPR）	ソフトウェアがデバイスのブートモード（DFU モードやリカバリモードなど）を追跡するために使用できる、SoC ハードウェアフラグのセット。 ブート・プログレス・レジスタ・フラグがいったんセットされると、クリアすることはできません。 そのため、 ソフトウェアは、 信頼できるシステム状態インジケータとしてこのフラグを使用できます。
Boot ROM	デバイスが起動したときに最初に実行されるコード。 プロセッサに不可欠な部分であるため、 Apple にも攻撃者にも変更できません。
データ保護	iOS 用のファイルおよびキーチェーン保護メカニズム。 App で使用される API を参照して、 ファイルおよびキーチェーン項目を保護することもできます。
デバイス・ファームウェア・アップグレード（DFU）	デバイスの Boot ROM のコードが USB 経由で復元されるまで待機するモード。 DFU モードのときは画面が真っ暗になりますが、「iTunes」 を実行しているコンピュータに接続すると、「iTunes はリカバリモードの iPad を見つけました。 iTunes でご利用になる前に、 この iPad を復元する必要があります。」 というメッセージが表示されます。
ECDSA	楕円曲線を用いた暗号方式に基づくデジタル署名アルゴリズム。
Effaceable Storage	暗号鍵を保存するために使用される NAND ストレージの専用領域。 直接アドレス指定でき、 安全にワイプできます。 攻撃者がデバイスを物理的に入手した場合は保護手段となりませんが、 Effaceable Storage に保存されている鍵を鍵階層の一部として使用することで、 高速のワイプと前方秘匿性を実現できます。
楕円曲線 Diffie-Hellman 鍵共有（ECDHE）	楕円曲線暗号を用いた Diffie-Hellman 方式での一時鍵の共有方法。 ECDHE では、 2 者間のメッセージを盗み見る第三者に鍵が発見されない方法で、 2 者が秘密鍵に同意できます。
Exclusive Chip Identification（ECID）	各 iOS デバイスのプロセッサに固有の 64 ビットの識別子。 1 台のデバイスで着信に応答すると、Bluetooth Low Energy 4.0 経由で短くアドバタイズすることで、 iCloud でペアリングされた近くにあるデバイスの着信音が停止します。 アドバタイズバイトは、 Handoff アドバタイズと同じ方法で暗号化されます。 パーソナライズプロセスの一部として使用され、 秘密とは見なされません。
ファイルシステム鍵	各ファイルのクラスキーなどのメタデータを暗号化する鍵です。 これは、 機密保持ではなく高速のワイプを可能にするために、 Effaceable Storage に保管されます。
グループ ID（GID）	UID と同じようなものですが、 クラス内のすべてのプロセッサで共通です。
ハードウェア・セキュリティ・モジュール（HSM）	デジタル鍵の保護および管理に特化した、 改ざん耐性を持つコンピュータ。
iBoot	セキュアブートチェーンの一部として XNU を読み込むコード。 SoC の世代に応じて、 LLB によって読み込まれるか、 または Boot ROM によって直接読み込まれます。
集積回路（IC）	マイクロチップとも呼ばれます。
Joint Test Action Group（JTAG）	プログラマや回路デベロッパが使用するハードウェアの標準デバッグツール。

キーバッグ	クラスキーのコレクションを保存するために使用されるデータ構造。 各タイプ（ユーザ、デバイス、システム、バックアップ、 エスクロー、 または iCloud バックアップ）のフォーマットは同じです。 • 以下を含むヘッダ ： – バージョン（iOS 5 では 3 に設定されます） – タイプ（システム、 バックアップ、 エスクロー、 または iCloud バックアップ） – キーバッグの UUID – HMAC（キーバッグが署名されている場合） – クラスキーのラッピングに使用される方式 ： UID とのタングル、 または PBKDF2 にソルトおよび反復回数を適用 • クラスキーのリスト ： – 鍵の UUID – クラス（ファイルまたはキーチェーンのデータ保護クラス） – ラッピングのタイプ（UID から導出された鍵のみ／ UID から導出された鍵とパスコードから導出された鍵） – ラップされたクラスキー – 非対称クラスの公開鍵
キーチェーン	パスワードや鍵、 機密性の高いその他の資格情報を保存したり取得したりするために iOS および他社製 App で使用されるインフラストラクチャおよび API セット。
鍵ラッピング	1 つの鍵を別の鍵で暗号化すること。 iOS では RFC 3394 準拠の NIST AES 鍵ラッピングが使用されます。
Low-Level Bootloader（LLB）	2 ステージ・ブート・アーキテクチャを実装したシステムで、 Boot ROM によって呼び出され、 セキュアブートチェーンの一部として iBoot を読み込むコード。
メモリコントローラ	ファイルシステム上のファイルの暗号化に使用される AES 256 ビット鍵。 Per File キーはクラスキーでラップされ、 ファイルのメタデータに保存されます。
Per File キー	ファイルシステム上のファイルの暗号化に使用される AES-256 ビット鍵。 Per File キーはクラスキーでラップされ、 ファイルのメタデータに保存されます。
プロビジョニングプロファイル	App を iOS デバイスにインストールしてテストできるようにする一連のエンティティおよびエンタイトルメントを含む、 Apple によって署名されたプロパティリスト。 開発プロビジョニングプロファイルにはデベロッパがアドホック配信用に選択したデバイスのリストが含まれ、 配信プロビジョニングプロファイルには企業によって開発された App の App ID が含まれます。
皮下の隆線角度のマッピング	指紋の一部から抽出されたリッジ（隆起部）の向きと幅を数学的に表現したもの。
ソフトウェア・シード・ビット	Secure Enclave の AES エンジンに実装され、 UID から鍵を生成する際に UID に追加される専用ビット。 各ソフトウェア・シード・ビットには、 対応するロックビットが含まれます。 Secure Enclave の Boot ROM と OS は、 対応するロックビットがセットされていない場合に限り、 各ソフトウェア・シード・ビットの値を独自に変更できます。 ロックビットの設定後は、 ソフトウェア・シード・ビットとロックビットのいずれも変更できません。 ソフトウェア・シード・ビットとロックビットは、 Secure Enclave の再起動時にリセットされます。
システムコプロセッサ整合性保護（SCIP）	アプリケーションプロセッサと同じ SoC 上にある CPU。
System on Chip（SoC）	複数のコンポーネントを 1 つのチップに組み込んだ集積回路（IC）。 SoC のコンポーネントには、 アプリケーションプロセッサ、 Secure Enclave、 その他のコプロセッサが含まれます。
タングル	ユーザのパスコードが暗号鍵に変換され、 デバイスの UID と組み合わせて強化されるプロセス。 これによって、 どのデバイスを侵害するにも総当たり（ブルートフォース）攻撃が必要になるため、 攻撃の速度が制限され、 攻撃を並列的に実行できなくなります。 タングルに使用されるアルゴリズムは PBKDF2 です。 このアルゴリズムの各反復では、 デバイス UID を鍵とする AES が擬似ランダム関数（PRF）として使用されます。
Uniform Resource Identifier（URI）	Web ベースのリソースを識別する文字列。
固有 ID（UID）	製造時に各プロセッサに焼き付けられる AES 256 ビット鍵。 ファームウェアまたはソフトウェアによって読み出すことはできず、 プロセッサのハードウェア AES エンジンによってのみ使用されます。 攻撃者が実際の鍵を取得するには、 プロセッサのシリコンに対して非常に高度でコストのかかる攻撃を仕掛ける必要があります。 UID は、 デバイス上にある UDID などのほかの識別子に関連しません。
XNU	iOS および macOS オペレーティングシステムの核心部にあるカーネル。 前提として信頼され、 コード署名、 サンドボックス化、 エンタイトルメントの確認、 ASLR などのセキュリティ対策を実行します。

改訂履歴

日付	概要
2018 年 11 月	**iOS 12.1 向けにアップデート** • グループ FaceTime
2018 年 9 月	**iOS 12 向けにアップデート** • Secure Enclave • OS 整合性保護 • 省電力モード対応のエクスプレスカード • DFU モードとリカバリモード • HomeKit 対応テレビ・リモコン・アクセサリ • 非接触型パス • 学生証 • Siri 検索候補 • Siri のショートカット •「ショートカット」App • ユーザパスワード管理 • スクリーンタイム • セキュリティ認定とプログラム
2018 年 7 月	**iOS 11.4 向けにアップデート** • 生体認証ポリシー • HomeKit • Apple Pay • ビジネスチャット • iCloud にメッセージを保管 • Apple Business Manager
2017 年 12 月	**iOS 11.2 向けにアップデート** • Apple Pay Cash **iOS 11.1 向けにアップデート** • セキュリティ認定とプログラム • Touch ID/Face ID • 共有メモ • CloudKit のエンドツーエンドの暗号化 • TLS • Apple Pay、Apple Pay による Web 上での支払い • Siri 検索候補 • 共有 iPad iOS 11 のセキュリティコンテンツについて詳しくは、次の Web サイトを参照してください。 support.apple.com/HT208112

日付	概要
2017 年 7 月	**iOS 10.3 向けにアップデート** • System Enclave • ファイルのデータ保護 • キーバッグ • セキュリティ認定とプログラム • SiriKit • HealthKit • ネットワークのセキュリティ • Bluetooth • 共有 iPad • 紛失モード • アクティベーションロック • プライバシーの制御 iOS 10.3 のセキュリティコンテンツについて詳しくは、次の Web サイトを参照してください。 support.apple.com/HT207617
2017 年 3 月	**iOS 10 向けにアップデート** • システムのセキュリティ • データ保護クラス • セキュリティ認定とプログラム • HomeKit、ReplayKit、SiriKit • Apple Watch • Wi-Fi、VPN • シングルサインオン • Apple Pay、Apple Pay による Web 上での支払い • クレジットカード、デビットカード、プリペイドカードのプロビジョニング • Safari 検索候補 iOS 10 のセキュリティコンテンツについて詳しくは、次の Web サイトを参照してください。 support.apple.com/HT207143
2016 年 5 月	**iOS 9.3 向けにアップデート** • 管理対象 Apple ID • Apple ID の 2 ファクタ認証 • キーバッグ • セキュリティの認証 • 紛失モード、アクティベーションロック • 保護したメモ • Apple School Manager、共有 iPad iOS 9.3 のセキュリティコンテンツについて詳しくは、次の Web サイトを参照してください。 support.apple.com/HT206166

日付	概要
2015 年 9 月	**iOS 9 向けにアップデート** • Apple Watch のアクティベーションロック • パスコードポリシー • Touch ID API のサポート • A8 でのデータ保護に AES-XTS を使用 • 自動ソフトウェア・アップデート用のキーバッグ • 証明書のアップデート • エンタープライズ App の信頼モデル • Safari ブックマークのデータ保護 • App Transport Security • VPN 仕様 • HomeKit 用の iCloud リモートアクセス • Apple Pay のポイントカード、Apple Pay のカード発行会社の App • Spotlight のデバイス上でのインデックス付け • iOS のペアリングモデル • Apple Configurator 2 • 機能制限 iOS 9 のセキュリティコンテンツについて詳しくは、次の Web サイトを参照してください。 support.apple.com/HT205212

2018 年 11 月