Appleプラットフォームのセキュリティ

2024年5月

目次

Appleプラットフォームのセキュリティの概要

Appleの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。Appleは世界で最も先進的なモバイルオペレーティングシステムを開発してきた経験を基に、モバイル、ウォッチ、デスクトップ、ホームに固有の要件に対応するセキュリティアーキテクチャを構築しました。

すべてのAppleデバイスでは、**ハードウェア**、**ソフトウェア**、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、個人情報の保護という究極の目的を果たすために、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。例えば、Appleが設計したシリコンやセキュリティハードウェアによって、重要なセキュリティ機能が強化されます。また、ソフトウェア保護によって、オペレーティングシステムと他社製アプリの安全性が保たれます。最後に、サービスによって、適切な時期にソフトウェアを安全にアップデートするためのメカニズムが提供され、アプリのエコシステムの安全性が高まり、通信や支払いが保護されます。結果として、Appleデバイス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。

Appleはシンプルかつ直観的で高性能な製品を設計するだけでなく、セキュリティを製品の設計に組み込んでいます。ハードウェアベースのデバイスの暗号化などの重要なセキュリティ機能は、誤って無効にできないようになっています。Face IDやTouch 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。これらのほとんどの機能はデフォルトで有効になっているため、ユーザまたはIT部門が何から何まで構成する必要はありません。

このドキュメントでは、Appleのプラットフォームにおいてセキュリティ技術やセキュリティ機能がどのように実装されているか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、Appleの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。

内容は、以下のトピックに分かれています。

- **ハードウェアセキュリティと生体認証:** Appleシリコン、Secure Enclave、暗号化エンジン、Face ID、Touch IDなど、Appleデバイスのセキュリティの基盤をなすシリコンやハードウェア
- **システムのセキュリティ:** 安全な起動、アップデート、およびAppleのオペレーティングシステムの継続的な動作を可能にする、統合されたハードウェア機能とソフトウェア機能
- **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、不正なユーザまたはプロセス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
- **アプリのセキュリティ:** アプリの安全なエコシステムを実現し、プラットフォームの整合性を損ねることなく安全にアプリを実行できるようにするソフトウェアおよびサービス
- **サービスのセキュリティ:** ID、パスワード管理、支払い、通信、紛失したデバイスの発見のためのAppleのサービス
- **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
- **デベロッパキットのセキュリティ:** プライバシーを守って家や健康を安全に管理するため、およびAppleのデバイスとサービスの機能を他社製アプリにまで拡張するためのフレームワークの「キット」
- **安全なデバイス管理:** Apple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

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。Appleセキュリティバウンティを設け、脆弱性を発見する研究者の取り組みを対象に報奨金の支払いを行っています。プログラムとバウンティのカテゴリについて詳しくは、https://security.apple.com/bounty/(英語)を参照してください。

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。さらに、セキュリティツールやトレーニングを提供し、脅威を積極的にモニタリングし、セキュリティ上の新しい問題をレポートしています。AppleはForum of Incident Response and Security Teams(FIRST)にも参加しています。

Appleの活動は、セキュリティを確保しプライバシーを保護するためにできることを押し広げていくことを目的としています。Appleでは、Apple Watchから、iPhoneやiPad、MacのMシリーズチップにわたる製品ラインナップで独自のAppleシリコンを利用することで、計算処理を効率化するだけでなく、セキュリティも強化しています。例えばAppleシリコンは、セキュアブート、Face IDとTouch ID、データ保護の基礎となっています。さらに、カーネル整合性保護、ポインタ認証コード、高速許可制限などのAppleシリコンを使用するセキュリティ機能によって、一般的な悪用を阻止することができます。そのため、攻撃者のコードが実行されてしまった場合でも、その攻撃による影響を大幅に軽減することができます。

Appleのプラットフォーム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、組織には自らのITポリシーとセキュリティポリシーを見直し、これら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技術を十分活かせるものにすることをおすすめします。

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、「セキュリティやプライバシーの脆弱性について報告する」を参照してください。

Appleはプライバシーを基本的人権と考え、アプリがユーザの情報を使用する方法と条件や、使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デバイスに組み込んでいます。プライバシー、Appleデバイスのプライバシー制御、およびAppleのプライバシーポリシーに対するAppleの取り組みについて詳しくは、https://www.apple.com/jp/privacy/を参照してください。

注記: 別途注意書きがない限り、このドキュメントでは次のバージョンのオペレーティングシステムを対象としています: iOS 17.3、iPadOS 17.3、macOS 14.3、tvOS 17.3、およびwatchOS 10.3。

ハードウェアセキュリティと生体認証

ハードウェアセキュリティの概要

保護する必要があるソフトウェアは、セキュリティが組み込まれているハードウェア上に置かれている必要があります。iOS、iPadOS、macOS、tvOS、およびwatchOSを搭載するAppleデバイスのシリコンにセキュリティ機能が埋め込まれているのは、そのためです。これらの機能には、システムセキュリティ機能を供給するCPUや、セキュリティ機能専用の追加のチップが含まれます。セキュリティに重点を置いたハードウェアは、攻撃対象領域を最小限に抑えるために、個別に定義された限定機能に対応するという原則に従います。このようなコンポーネントには、セキュアブートのハードウェア信頼ルートを形成するBoot ROM、効率的で安全な暗号化と復号のための専用AESエンジン、およびSecure Enclaveなどがあります。**Secure Enclave**はAppleのSystem on Chip（SoC）のコンポーネントです。これは、iPhone、iPad、Apple Watch、Apple TV、HomePodデバイスのすべての最新モデルと、Appleシリコン搭載MacおよびApple T2セキュリティチップ搭載Macのすべてに含まれています。Secure Enclave自体はSoCと同じ設計原則に従い、独自のディスクリートBoot ROMおよびAESエンジンを持ちます。Secure Enclaveは、保存されたデータの暗号化に必要な鍵の安全な生成と保存の基盤も提供し、Face IDとTouch IDの生体認証データを保護および評価します。

ストレージの暗号化は、高速かつ効率的に処理する必要があります。同時に、暗号鍵の関係を構築する際に使用するデータ（または**鍵マテリアル**）が公開されることも防ぐ必要があります。AESハードウェアエンジンは、**ファイルの書き込みまたは読み取り時に**高速のインライン暗号化と復号を実行することにより、この問題を解決します。Secure Enclaveからの特殊なチャネルは、この情報をアプリケーションプロセッサ（またはCPU）またはオペレーティングシステム全体に公開することなく、必要な鍵マテリアルをAESエンジンに提供します。そのため、存続期間の長い暗号鍵を公開することなく、Appleのデータ保護およびFileVaultテクノロジーによってユーザのファイルを保護できます。

Appleが設計したセキュアブートは、最下位レベルのソフトウェアを改ざんから保護し、Appleから提供された信頼できるオペレーティングシステムソフトウェアのみが起動時に読み込まれるようにするためのものです。セキュアブートは、Apple SoC製造時に書き込まれる**Boot ROM**という変更不可のコードから始まります。このコードは**ハードウェア信頼ルート**とも呼ばれます。T2チップを搭載したMacコンピュータでは、T2がmacOSのセキュアブートの信頼の起点になります。（T2チップとSecure Enclaveは、どちらも独自の別々のBoot ROMを使用して独自のセキュアブートプロセスを実行します。これは、Aシリーズ、M1、M2のチップが安全にブートする方法とまったく同じです。）

Secure Enclaveは、AppleデバイスでFace IDおよびTouch IDセンサーからの顔および指紋データも処理します。これにより、ユーザの生体認証データのプライバシーとセキュリティを確保しながら、安全に認証できます。さらに、アクセス時や購入時などの多くの状況下で、長く複雑なパスコードおよびパスワードと同等のセキュリティを保ちながら、素早く簡単にユーザを認証できるようになります。

Apple SoCのセキュリティ

Appleが設計したシリコンはすべてのApple製品に共通するアーキテクチャを形成し、今やiPhone、iPad、Apple TV、Apple Watchだけでなく、Macにも搭載されています。10年以上にわたり、Appleの世界トップクラスのシリコン設計チームはApple SoC（System on Chip）の構築と改良を行ってきました。その成果は、すべてのデバイス向けに設計されたスケーラブルなアーキテクチャに結実し、セキュリティ能力の面において業界を牽引してきました。このようなセキュリティ機能の共通基盤は、ソフトウェアと連携するように独自のシリコンを設計する企業だからこそ実現できるものです。

Appleシリコンは、以下に示すシステムセキュリティ機能を可能とするために設計、製造されています:

機能	A10	A11、S3	A12、A13、A14 S4–S9	A15、A16、A17	M1、M2、M3
カーネル整合性保護	✓	✓	✓	✓	✓
高速許可制限	✗	✓	✓	✓	✓
システムコプロセッサ整合性保護	✗	✗	✓	✓	✓
ポインタ認証コード	✗	✗	✓	✓	✓
ページ保護レイヤー	✗	✓	✓	✗	✗ 以下の注記1を参照。
Secure Page Table Monitor	✗	✗	✗	✓ 以下の注記2を参照。	✗

注記1: ページ保護レイヤー（PPL）では、プラットフォームが署名済みの信頼できるコード**のみを**実行する必要があります。このセキュリティモデルは、macOSには該当しません。

注記2: SPTM（Secure Page Table Monitor）はA15、A16、およびA17で対応していて、対応するプラットフォームでページ保護レイヤーに代わるものです。

Appleが設計したシリコンは、以下に示すデータ保護機能も可能にします。

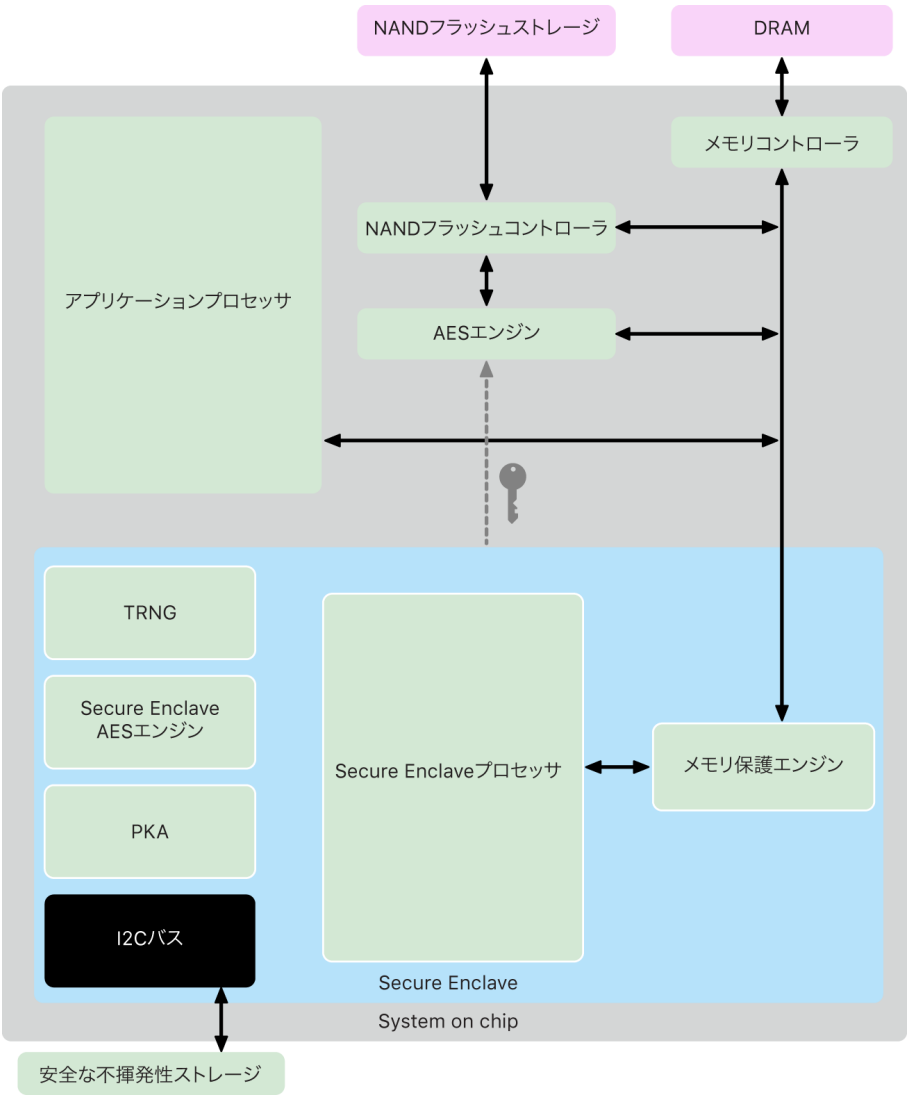
機能	A10、A11 S3	A12–A17 S4–S9 M1、M2、M3
シールドキー保護（SKP）	✓	✓
recoveryOS - 保護されているすべてのデータ保護クラス	✓	✓
DFUの代替起動、Diagnostics、およびアップデート - 保護されているクラスA、B、およびCのデータ	✗	✓

Secure Enclave

Secure Enclaveは最新バージョンのiPhone、iPad、Mac、Apple TV、Apple Watch、およびHomePod専用セキュアサブシステムです。

概要

Secure Enclaveは、AppleのSystem on Chip（SoC）に組み込まれた専用のセキュリティサブシステムです。Secure Enclaveはセキュリティ層を追加するためにメインプロセッサから隔離されており、アプリケーションプロセッサのカーネルが侵害された場合でも、ユーザの機密データを安全に保てるように設計されています。Secure EnclaveはSoCと同じ設計原則に従っており、ハードウェア信頼ルートを確立するためのBoot ROM、効率的で安全な暗号化操作のためのAESエンジン、および保護されたメモリを備えています。Secure Enclaveにはストレージは含まれていませんが、アプリケーションプロセッサとオペレーティングシステムで使用されるNANDフラッシュストレージとは別の接続されたストレージに、情報を安全に保存するメカニズムがあります。



Secure EnclaveはほとんどのバージョンのiPhone、iPad、Mac、Apple TV、Apple Watch、およびHomePodに備わるハードウェア機能です。以下のモデルに搭載されています:

- iPhone 5s以降
- iPad Air以降
- Appleシリコン搭載Macコンピュータ
- Apple T1チップを搭載した、Touch Bar搭載MacBook Proコンピュータ(2016および2017)
- Apple T2セキュリティチップを搭載した、Intelプロセッサ搭載Macコンピュータ
- Apple TV HD以降
- Apple Watch Series 1以降
- HomePodおよびHomePod mini

Secure Enclaveプロセッサ

Secure EnclaveプロセッサはSecure Enclaveのための主要な演算能力を提供します。最大限の隔離を実現するために、Secure EnclaveプロセッサはSecure Enclave専用となっています。これにより、攻撃を受けているソフトウェアと同じ実行コアを共有中の悪意のあるソフトウェアに依存したサイドチャネル攻撃を防止することができます。

Secure EnclaveプロセッサはAppleがカスタマイズしたL4マイクロカーネルのバージョンを実行します。これは低いクロック速度でも効率的に動作するよう設計されており、クロック攻撃や電力攻撃を受けても保護されます。Secure Enclaveプロセッサ(A11およびS4以降)には、メモリ保護エンジン、アンチリプレイ機能を持つ暗号化メモリ、セキュアブート、専用の乱数ジェネレータ、および独自のAESエンジンが搭載されています。

メモリ保護エンジン

Secure EnclaveはデバイスのDRAMメモリの専用領域から動作します。複数の保護層がSecure Enclaveで保護されたメモリをアプリケーションプロセッサから隔離します。

デバイスが起動すると、Secure Enclave Boot ROMによってメモリ保護エンジン用の一時的なランダムメモリ保護鍵が作成されます。Secure Enclaveが専用メモリ領域に書き込むときには、AESをMac XEX(xor-encrypt-xor)モードで使用しているメモリブロックをメモリ保護エンジンが暗号化し、メモリ用にCMAC(Cipher-based Message Authentication Code)認証タグを計算します。メモリ保護エンジンは暗号化されたメモリと共に認証タグを保存します。Secure Enclaveがメモリを読み込むときには、メモリ保護エンジンが認証タグを検証します。認証タグが一致する場合は、メモリ保護エンジンがメモリブロックを復号します。タグが一致しない場合は、メモリ保護エンジンがSecure Enclaveにエラーを送信します。メモリ認証エラーが発生すると、システムがリブートするまでSecure Enclaveはリクエストを受け付けなくなります。

Apple A11やS4 SoCから、メモリ保護エンジンはSecure Enclaveメモリ用のリプレイ保護を追加します。セキュリティ上重要なデータのリプレイを防止するために、メモリ保護エンジンは認証タグと共にメモリブロック用の**アンチリプレイ値**と呼ばれる一意の使い捨ての番号を保存します。アンチリプレイ値はCMAC認証タグ用の追加の微調整として使用されます。すべてのメモリブロック用のアンチリプレイ値は、Secure Enclave内の専用SRAMをルートとする整合性ツリーを使用して保護されます。書き込み時には、メモリ保護エンジンはアンチリプレイ値および整合性ツリーの各レベルをSRAMまで**アップデート**します。読み込み時には、メモリ保護エンジンはアンチリプレイ値および整合性ツリーの各レベルをSRAMまで**検証**します。アンチリプレイ値の不一致は認証タグの不一致と同様に扱われます。

Apple A14、M1、またはそれ以降のSoCでは、メモリ保護エンジンは2つの一時的なメモリ保護鍵に対応します。1つはSecure Enclave専用のデータに使用され、もう1つはSecure Neural Engineと共有されるデータに使用されます。

メモリ保護エンジンはSecure Enclaveに対してインラインで透過的に動作します。Secure Enclaveがメモリの読み込みと書き込みを行うときは、それが通常の暗号化されていないDRAMであるかのように行います。一方、Secure Enclaveの外側にいるオブザーバには、メモリの暗号化され認証されたバージョンしか見えません。つまり、パフォーマンスが低下したりソフトウェアが複雑化したりすることなく、強力なメモリ保護が提供されます。

Secure Enclave Boot ROM

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。

システム起動時に、iBootはSecure Enclaveにメモリの専用領域を割り当てます。Secure Enclave Boot ROMは、メモリを使用する前に、メモリ保護エンジンを初期化して、Secure Enclaveで保護されたメモリを暗号化によって保護します。

次に、アプリケーションプロセッサがsepOSイメージをSecure Enclave Boot ROMに送信します。sepOSイメージをSecure Enclaveで保護されたメモリにコピーしたあと、Secure Enclave Boot ROMは暗号学的ハッシュとイメージの署名をチェックし、sepOSがデバイス上での実行を承認されていることを検証します。sepOSイメージがデバイス上で実行されることに関して適切に署名されている場合は、Secure Enclave Boot ROMは制御権をsepOSに移転します。Secure Enclave Boot ROMは、署名が無効な場合に、次にチップがリセットされるまでSecure Enclaveの使用を防止するように設計されています。

Apple A10以降のSoCでは、Secure Enclave Boot ROMはsepOSのハッシュを専用のレジスタにロックします。公開鍵アクセラレータはこのハッシュをオペレーティングシステム固定（OS固定）鍵に使用します。

Secure Enclave Boot Monitor

Apple A13以降のSoCでは、ブートされたsepOSのハッシュで整合性を強化するためのブートモニタがSecure Enclaveに含まれています。

システム起動時には、Secure Enclaveプロセッサのシステムコプロセッサ整合性保護（SCIP）構成によって、Secure Enclaveプロセッサが Secure Enclave Boot ROM以外のコードを実行することを防止できます。ブートモニタはSecure EnclaveがSCIP構成を直接変更することを防止します。読み込まれたsepOSを実行可能とするために、Secure Enclave Boot ROMはブートモニタにリクエストを送信します。このとき、読み込まれたsepOSのアドレスとサイズも送信されます。リクエストを受信したブートモニタはSecure Enclaveプロセッサをリセットし、読み込まれたsepOSをハッシュ化し、読み込まれたsepOSの実行を許可するようにSCIP設定をアップデートし、新しく読み込まれたコード内で実行を開始します。システムがブートしている間は、新しいコードが実行可能となるたびにこの同じプロセスが実行されます。そのたびに、ブートモニタはブートプロセスの実行中ハッシュをアップデートします。ブートモニタは、実行中ハッシュ内の重要なセキュリティパラメータも取り込みます。

ブートが完了すると、ブートモニタは実行中ハッシュをファイナライズして、OS固定鍵に使用できるように公開鍵アクセラレータに送信します。このプロセスの設計により、たとえSecure Enclave Boot ROMに脆弱性があっても、オペレーティングシステム鍵固定がバイパスされることはありません。

真性乱数生成器

真性乱数生成器（TRNG）は安全なランダムデータを生成するのに使用されます。Secure Enclaveがランダムな暗号鍵、ランダムな鍵シードなどのエントロピーを生成するたびにTRNGが使用されます。TRNGは、CTR_DRBG（カウンタモードのブロック暗号に基づくアルゴリズム）で後処理された複数のリングオシレータに基づいています。

ルート暗号鍵

Secure EnclaveはユニークID（UID）のルート暗号鍵を備えています。UIDはデバイスごとに一意であり、デバイス上のそれ以外のいかなる識別子にも結びついていません。

SoCの製造時、ランダム生成されたUIDがヒューズに書き込まれます。A9 SoC以降、UIDは製造中にSecure Enclave TRNGによって生成され、完全にSecure Enclaveで実行されるソフトウェアプロセスを使用してヒューズに書き込まれます。このプロセスにより、製造中にUIDがデバイスの外部からは見えなくなり、Appleやそのサプライヤがアクセスしたり保存したりすることはできません。

sepOSはデバイス固有のシークレットを保護するためにUIDを使用します。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。例えば、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、内蔵SSDストレージ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。保護されるその他のデバイス固有のシークレットとしては、Face IDまたはTouch IDのデータがあります。Macでは、AESエンジンにリンクされた完全に内部のストレージのみがこのレベルの暗号化を受け取ります。例えば、USBで接続された外部ストレージデバイスも、Mac Pro（2019）に追加されたPCIeベースのストレージも、この方法では暗号化されません。

また、Secure Enclaveにはデバイスグループ ID（GID）があり、これは同じSoCを搭載しているすべてのデバイスに共通しています（例えば、Apple A15 SoCを使用しているすべてのデバイスは同じGIDを共有しています）。

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アクセスすることはできません。

Secure Enclave AESエンジン

Secure Enclave AESエンジンとは、AES暗号に基づいた対称暗号を実行するために使用されるハードウェアブロックです。AESエンジンは、タイミングと静的電力解析（SPA）を使用して、情報漏えいに耐えうるように設計されています。A9 SoCから、AESエンジンは動的電力解析（DPA）への対策も備えています。

AESエンジンはハードウェア鍵とソフトウェア鍵をサポートします。ハードウェア鍵はSecure EnclaveのUIDまたはGIDから導出されます。これらの鍵はAESエンジンの内部にとどまり、sepOSソフトウェアからも見ることはできません。ソフトウェアはハードウェア鍵を使用した暗号化と復号をリクエストできますが、鍵を抜き出すことはできません。

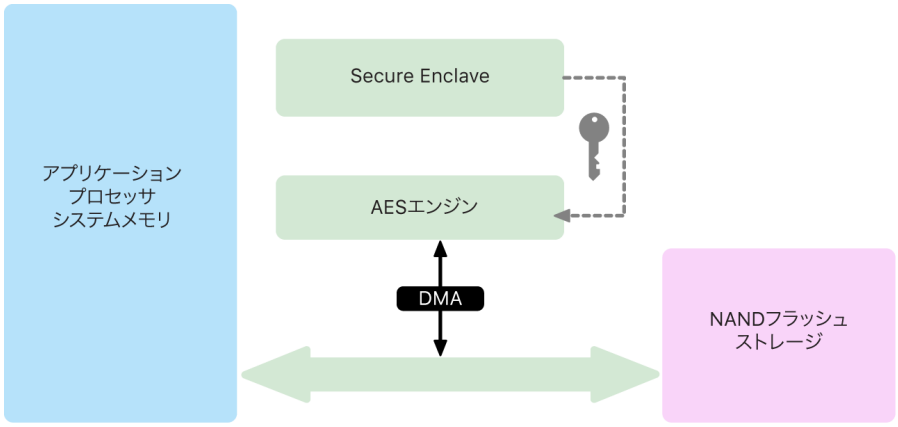
Apple A10以降のSoCsでは、AESエンジンに、UIDまたはGIDから導出された鍵を多様化させるためのロック可能なシードビットが含まれています。これによって、デバイスの動作モードに応じてデータアクセスを制限できるようになります。ロック可能なシードビットは、デバイスファームウェアアップデート（DFU）モードからブートするときにパスワード保護されたデータへのアクセスを拒否するときなどに使用されます。詳しくは、パスコードとパスワードを参照してください。

AESエンジン

Secure Enclaveを備えたすべてのAppleデバイスには、NAND（不揮発性）フラッシュストレージとシステムのメインメモリ間の直接メモリアクセス（DMA）パスに専用のAES256の暗号化エンジン（「AESエンジン」）も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DMA暗号化エンジン経由でのアクセスのみ許可されます。

ブート時には、sepOSがTRNGを使用して一時的なキーラッピング鍵を生成します。Secure Enclaveは、Secure Enclaveの外部にあるソフトウェアからアクセスされることを防止するための専用ワイヤを使ってこの鍵をAESエンジンに伝送します。sepOSはその後、アプリケーションプロセッサのファイルシステムドライバによって使用されるファイルキーを、一時的なラッピング鍵を使ってラップします。ファイルシステムドライバがファイルを読み込んだり書き込んだりするときには、ラッピングされた鍵をAESエンジンに送信し、AESエンジンが鍵をラッピング解除します。AESエンジンがアンラップされた鍵をソフトウェアに公開することはありません。

注記: AESエンジンはSecure EnclaveおよびSecure Enclave AESエンジンのどちらとも別個のコンポーネントですが、その動作は、以下に示すようにSecure Enclaveと密接に関連しています。



公開鍵アクセラレータ

公開鍵アクセラレータ（PKA）は非対称暗号演算を実行するのに使用されるハードウェアブロックです。PKAはRSAおよびECC（楕円曲線暗号）署名および暗号化アルゴリズムをサポートします。PKAは、SPAやDPAなどのタイミング攻撃やサイドチャネル攻撃による情報漏えいに耐えうるように設計されています。

PKAはソフトウェア鍵とハードウェア鍵をサポートします。ハードウェア鍵はSecure EnclaveのUIDまたはGIDから導出されます。これらの鍵はPKAの内側にとどまり、sepOSソフトウェアからも見ることはできません。

A13 SoC以降、PKAの暗号化の実装は、正式な検証手法を使用して数学的に正しいことが証明されています。

Apple A10以降のSoCでは、PKAは、シールドキー保護（SKP）とも呼ばれるOS固定鍵をサポートします。これらの鍵は、デバイスのUIDとデバイス上で実行されているsepOSのハッシュの組み合わせを使用して生成されます。ハッシュはSecure Enclave Boot ROMから提供されます。または、Apple A13以降のSoC上のSecure Enclave Boot Monitorから提供されます。これらの鍵は、特定のAppleサービスにリクエストを送信するときにsepOSバージョンを検証するためにも使用されます。また、ユーザの承認なしでシステムに重大な変更が加えられた場合に鍵マテリアルへのアクセスを防ぐことで、パスコードで保護されたデータのセキュリティを向上させるためにも使用されます。

セキュア不揮発性ストレージ

Secure Enclaveは、専用のセキュア不揮発性ストレージデバイスを備えています。セキュア不揮発性ストレージは専用のI2Cバスを通してSecure Enclaveに接続されているため、Secure Enclaveからしかアクセスできないようになっています。すべてのユーザデータ暗号鍵は、Secure Enclaveの不揮発性ストレージに保存されているエントロピーに基づいています。

A12、S4、またはそれ以降のSoCを搭載したデバイスでは、Secure Enclaveがエントロピーストレージ用のセキュアストレージコンポーネントとペアリングされます。セキュアストレージコンポーネント自体は、変更不可のROMコード、ハードウェア乱数ジェネレータ、デバイスごとの一意の暗号鍵、暗号化エンジン、および物理的改ざん検出機能を備えて設計されています。Secure Enclaveとセキュアストレージコンポーネントは、暗号化および認証されたプロトコルを使用して通信しており、これによってエントロピーに排他的にアクセスできます。

2020年秋以降に初めてリリースされたデバイスは第2世代のセキュアストレージコンポーネントを搭載しています。第2世代のセキュアストレージコンポーネントにはカウンタロックボックスが追加されています。カウンタロックボックスにはそれぞれ、128ビットのソルト、128ビットのパスコードベリファイア、8ビットカウンタ、8ビット最大試行値が保存されています。カウンタロックボックスには、暗号化および認証されたプロトコルを使ってアクセスします。

カウンタロックボックスは、パスコードで保護されたユーザデータのロックを解除するために必要なエントロピーを保持します。このユーザデータにアクセスするには、ペアリングされたSecure EnclaveがユーザのパスコードとSecure EnclaveのUIDから正しいパスコードエントロピー値を導出する必要があります。ペアリングされたSecure Enclave以外のソースから送信されたロック解除試行によって、ユーザのパスコードが学習されることはありません。パスコードの最大試行回数（例えば、iPhoneの場合は10回）を超えると、パスコードで保護されているデータがセキュアストレージコンポーネントによって完全に消去されます。

カウンタロックボックスを作成するために、Secure Enclaveはセキュアストレージコンポーネントにパスコードエントロピー値と最大試行値を送信します。セキュアストレージコンポーネントは、乱数ジェネレータを使用してソルト値を生成します。そのあと、提供されたパスコードエントロピー、セキュアストレージコンポーネントの一意の暗号鍵、およびソルト値から、パスコードベリファイア値とロックボックスエントロピー値を導出します。セキュアストレージコンポーネントは、カウント0、提供された最大試行値、導出されたパスコードベリファイア値、およびソルト値でカウンタロックボックスを初期化します。次に、セキュアストレージコンポーネントは生成されたロックボックスエントロピー値をSecure Enclaveに返します。

あとでロックボックスエントロピー値をカウンタロックボックスから取り戻すために、Secure Enclaveはセキュアストレージコンポーネントにパスコードエントロピーを送信します。セキュアストレージコンポーネントは最初にロックボックスのカウンタを増分します。増分されたカウンタが最大試行値を超えた場合、セキュアストレージコンポーネントはカウンタロックボックスを完全に消去します。最大試行回数に達していない場合、セキュアストレージコンポーネントは、カウンタロックボックスの作成に使用されたのと同じアルゴリズムを使用して、パスコードベリファイア値とロックボックスエントロピー値の導出を試みます。導出されたパスコードベリファイア値が保存されているパスコードベリファイア値と一致する場合、セキュアストレージコンポーネントはロックボックスエントロピー値をSecure Enclaveに返し、カウンタを0にリセットします。

パスワード保護されたデータにアクセスするために使用される鍵は、カウンタロックボックスに格納されたエントロピーに基づいています。詳しくは、データ保護の概要を参照してください。

安全な不揮発性ストレージは、Secure Enclave内のすべてのアンチリプレイサービスに使用されます。Secure Enclaveのアンチリプレイサービスは、アンチリプレイ境界をマークするイベントを介したデータの失効に使用されます。これには以下のものが含まれますが、これらに限定されません:

- パスコードの変更
- Face IDまたはTouch IDの有効化または無効化
- Face IDの顔またはTouch IDの指紋の追加または削除
- Face IDまたはTouch IDのリセット
- Apple Payカードの追加または削除
- すべてのコンテンツと設定の消去

セキュアストレージコンポーネントを備えていないアーキテクチャでは、EEPROM(電気的に消去可能なプログラマブル読み取り専用メモリ)を使用して、Secure Enclaveに安全なストレージサービスを提供します。セキュアストレージコンポーネントと同様に、EEPROMは接続されているSecure Enclaveからのみアクセスできますが、専用のハードウェアセキュリティ機能は含まれていません。また、エントロピー(物理的な接続特性を除く)への排他的アクセスやカウンタロックボックス機能も保証していません。

Secure Neural Engine

Touch IDではなくFace IDを搭載したデバイスでは、Secure Neural Engineは2D画像と深度マップをユーザの顔の数学的モデルに変換します。

A11からA13 SoCsでは、Secure Neural EngineはSecure Enclaveに組み込まれています。Secure Neural Engineはパフォーマンス向上のためにダイレクトメモリアクセス(DMA)を使用します。sepOSカーネルの制御下にあるIOMMU(入出力メモリ管理ユニット)は、この直接アクセスを承認済みのメモリ領域に制限します。

A14、M1、またはそれ以降、Secure Neural Engineはアプリケーションプロセッサの Neural Engineのセキュアモードとして実装されています。専用ハードウェアセキュリティコントローラがアプリケーションプロセッサとSecure Enclaveのタスクを切り替えて、各トランザクションでNeural Engineの状態をリセットしてFace IDのデータの安全性を保ちます。専用エンジンは、メモリ暗号化、認証、およびアクセス制御を利用します。同時に、別々の暗号鍵とメモリ範囲を使用して、Secure Neural Engineを承認済みのメモリ領域に制限します。

電力とクロックのモニタ

すべての電子機器は限られた電圧と周波数の範囲内で動作するように設定されています。この範囲外での動作では電子機器が誤動作する可能性があり、セキュリティ制御がバイパスされる可能性があります。電圧と周波数が安全な範囲内から外れないようにするため、Secure Enclaveは監視回路と連携するように設計されています。これらの監視回路は、Secure Enclaveよりもはるかに大きな動作範囲を持つように設計されています。モニタが不正な動作点を検出した場合、Secure Enclaveのクロックは自動的に停止し、次のSoCリセットまで再開しません。

Secure Enclave機能の概要

注記: 2020年秋に初めてリリースされたA12、A13、S4、およびS5製品は第2世代のセキュアストレージコンポーネントを搭載していますが、同じSoCに基づくそれ以前の製品は第1世代のセキュアストレージコンポーネントを搭載しています。

SoC	メモリ保護エンジン	セキュアストレージ	AESエンジン	PKA
A8	暗号化と認証	EEPROM	あり	なし
A9	暗号化と認証	EEPROM	DPA保護	あり
A10	暗号化と認証	EEPROM	DPA保護とロック可能なシードビット	OS固定鍵
A11	暗号化、認証、リプレイ防止	EEPROM	DPA保護とロック可能なシードビット	OS固定鍵
A12（2020年秋より前にリリースされたAppleデバイス）	暗号化、認証、リプレイ防止	セキュアストレージコンポーネント第1世代	DPA保護とロック可能なシードビット	OS固定鍵
A12（2020年秋よりあとにリリースされたAppleデバイス）	暗号化、認証、リプレイ防止	セキュアストレージコンポーネント第2世代	DPA保護とロック可能なシードビット	OS固定鍵
A13（2020年秋より前にリリースされたAppleデバイス）	暗号化、認証、リプレイ防止	セキュアストレージコンポーネント第1世代	DPA保護とロック可能なシードビット	OS固定鍵とブートモニタ
A13（2020年秋よりあとにリリースされたAppleデバイス）	暗号化、認証、リプレイ防止	セキュアストレージコンポーネント第2世代	DPA保護とロック可能なシードビット	OS固定鍵とブートモニタ
A14–A17	暗号化、認証、リプレイ防止	セキュアストレージコンポーネント第2世代	DPA保護とロック可能なシードビット	OS固定鍵とブートモニタ
S3	暗号化と認証	EEPROM	DPA保護とロック可能なシードビット	あり
S4	暗号化、認証、リプレイ防止	セキュアストレージコンポーネント第1世代	DPA保護とロック可能なシードビット	OS固定鍵
S5（2020年秋より前にリリースされたAppleデバイス）	暗号化、認証、リプレイ防止	セキュアストレージコンポーネント第1世代	DPA保護とロック可能なシードビット	OS固定鍵
S5（2020年秋よりあとにリリースされたAppleデバイス）	暗号化、認証、リプレイ防止	セキュアストレージコンポーネント第2世代	DPA保護とロック可能なシードビット	OS固定鍵
S6–S9	暗号化、認証、リプレイ防止	セキュアストレージコンポーネント第2世代	DPA保護とロック可能なシードビット	OS固定鍵
T2	暗号化と認証	EEPROM	DPA保護とロック可能なシードビット	OS固定鍵
M1、M2、M3	暗号化、認証、リプレイ防止	セキュアストレージコンポーネント第2世代	DPA保護とロック可能なシードビット	OS固定鍵とブートモニタ

Face IDとTouch ID

Face IDとTouch IDのセキュリティ

パスコードとパスワードはAppleデバイスのセキュリティにとって非常に重要です。同時に、ユーザはデバイスに1日100回以上アクセスすることも多いため、デバイスへのアクセスの利便性も確保する必要があります。生体認証により、強力なパスコードでセキュリティを維持（または、手動で入力する必要がないためパスコードまたはパスワードを強力なものに変更）しつつ、指で一押しするかデバイスに顔を向けるだけで迅速にロック解除できる利便性も実現されます。Face IDとTouch IDはパスコードやパスワードに取って代わるものではありませんが、ほとんどの状況でアクセスをより速く、より簡単にします。

Appleの生体認証セキュリティアーキテクチャは、生体認証センサーとSecure Enclaveの責任の厳密な分離と、両者の安全な接続に依存しています。センサーは生体認証イメージを取り込み、それを安全にSecure Enclaveに伝送します。登録時には、対応するFace IDおよびTouch IDのテンプレートデータをSecure Enclaveが処理し、暗号化して保存します。照合時には、Secure Enclaveが生体認証センサーから受信したデータを保存済みのテンプレートと比較し、デバイスのロック解除、または一致が有効であるという応答（Apple Pay、アプリ内、またはFace IDおよびTouch IDのその他の用途の場合）を行うかどうかを決定します。このアーキテクチャは、センサーとSecure Enclaveの両方を備えたデバイス（iPhone、iPadや多くのMacシステム）と、センサーを物理的に分離してペリフェラルに組み込み、Appleシリコン搭載MacのSecure Enclaveに安全にペアリングできる環境に対応します。

Face IDのセキュリティ

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ユーザの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、ユーザがデバイスを見つめるだけでロックを解除でき、対応するデバイスではマスクを付けたままでも可能です。Face IDは、外見の変化に自動的に適応し、ユーザの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ります。

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デバイスのスリープを解除する（デバイスを持ち上げるか画面をタップする）際や、着信通知を表示するためにこれらのデバイスがユーザの認証を要求する際、または対応するアプリが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Face IDによって確認され、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では、Face IDの注視認識はVoiceOverが有効なときは無効になります。また、必要に応じて別途無効にすることもできます。マスクを付けてFace IDを使用する場合は常に注視検出が必要です。

TrueDepthカメラによってユーザが注視していることが確認されると、数千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Secure Neural Engine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ユーザの顔のデータの数学的モデルです。

Touch IDのセキュリティ

Touch IDは、対応Appleデバイス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。

Touch IDセンサーを搭載したAppleデバイスは、指紋を使ってロックを解除できます。Touch IDは、デバイスパスコードまたはユーザパスワードのニーズに代わるものではありません。デバイスの起動、再起動、またはログアウト(Macの場合)の後には、従来通りパスコードまたはパスワードが必要です。一部のアプリでは、Touch IDをデバイスパスコードまたはユーザパスワードの代わりに使用することもできます。例えば、メモアプリのパスワードで保護されたメモ、キーチェーンで保護されたWebサイトや、Touch ID対応のアプリのパスワードのロックを解除するために使用します。ただし、一部のシナリオでは、デバイスのパスコードまたはユーザのパスワードが常に必要です(例えば、既存のデバイスのパスコードやユーザのパスワードを変更したり、既存の指紋登録を削除したり、新しい指紋登録を作成したりする場合です)。

指紋センサーで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。この接続を保護するために使用されるチャネルは、Touch IDセンサーがSecure Enclaveを備えたデバイスに内蔵されているか、別個のペリフェラル上にあるかによって異なります。

ラスター形式のこのスキャン結果は、解析用に指紋スキャンが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。登録時に、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ます。Secure Enclaveのみが、今後の照合で比較対象にするテンプレートとして、これを読み取ることができます。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。

内蔵Touch IDのチャネルのセキュリティ

Secure Enclaveと内蔵Touch IDセンサーの間の通信は、シリアルペリフェラルインターフェイスバス経由で行われます。プロセッサはデータをSecure Enclaveに転送しますが、データ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。どのTouch IDセンサーでも、共有鍵は強力かつランダムであり、同じものはありません。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ることにより、認証と機密保護の両方が実現します。

Touch ID搭載Magic Keyboard

Touch ID搭載Magic Keyboard（およびテンキー付きTouch ID搭載Magic Keyboard）は、すべてのAppleシリコン搭載Macで使用できる外部キーボードにTouch IDセンサーを備えたものです。Touch ID搭載Magic Keyboardは生体認証センサーの役割を果たします。生体認証テンプレートの保存、生体認証の照合、セキュリティポリシー（ロックを解除せずに48時間経過するとパスワードの入力が必要になるなど）の適用は行いません。Touch ID搭載Magic KeyboardのTouch IDセンサーを使用するには、MacのSecure Enclaveと安全にペアリングする必要があります。その後、内蔵Touch IDセンサーの場合と同様に、Secure Enclaveが登録と照合を行い、セキュリティポリシーを適用します。Macに同梱のTouch ID搭載Magic Keyboardの場合は、Appleが工場でペアリングプロセスを実行します。必要に応じて、ユーザがペアリングを行うこともできます。Touch ID搭載Magic Keyboardは一度に1台のMacとのみ安全にペアリングできますが、Macは最大5台の異なるTouch ID搭載Magic Keyboardと安全なペアリングを維持できます。

Touch ID搭載Magic Keyboardは内蔵Touch IDセンサーと互換性があります。Macの内蔵Touch IDセンサーで登録した指がTouch ID搭載Magic Keyboardで提示された場合、MacのSecure Enclaveが照合を正常に処理できます。逆の場合も同様です。

MacのSecure EnclaveとTouch ID搭載Magic Keyboardの安全なペアリングとその後の通信をサポートするため、このキーボードは証明のための公開鍵アクセラレータ（PKA）ブロックと、必要な暗号化プロセスを実行するためのハードウェアベースの鍵を備えています。

安全なペアリング

Touch ID搭載Magic KeyboardをTouch ID操作に使用するには、キーボードをMacに安全にペアリングする必要があります。ペアリングのために、MacのSecure EnclaveとTouch ID搭載Magic KeyboardのPKAブロックが、Appleの信頼できるCAをルートとする公開鍵を交換し、ハードウェアに保持されている証明鍵と一時的なECDHを使用して自らの識別情報を証明します。このデータは、MacではSecure Enclave、Touch ID搭載Magic KeyboardではPKAブロックによって保護されます。安全にペアリングしたあとは、MacとTouch ID搭載Magic Keyboardの間で通信されるすべてのTouch IDデータが、保存されている識別情報に基づくNIST P-256曲線を用いた一時ECDH鍵を使用して、鍵長256ビットのAES-GCMによって暗号化されます。ワイヤレスモードでのキーボードの使用について詳しくは、Bluetoothのセキュリティを参照してください。

ペアリングのセキュアインテント

新しい指紋の登録などの一部のTouch ID操作を初めて行うときは、ユーザがTouch ID搭載Magic KeyboardをMacと一緒に使用する意図を物理的に確認する必要があります。物理的な意図の確認は、ユーザインターフェイスによって指示されたときにMacの電源ボタンを2回押す操作、または以前にMacに登録した指紋との一致によって行われます。詳しくは、セキュアインテントとSecure Enclaveへの接続を参照してください。

Apple Payのトランザクションは、Touch IDでの一致、またはmacOSのユーザパスワードを入力してTouch ID搭載Magic KeyboardのTouch IDボタンを2回押す操作で承認できます。後者の場合は、ユーザがTouch IDでの照合を行わなくても物理的に意図を確認できます。

Touch ID搭載Magic Keyboardのチャネルのセキュリティ

Touch ID搭載Magic KeyboardのTouch IDセンサーと、ペアリングされているMacのSecure Enclaveの間に安全な通信チャネルを確保するには、以下のものが必要です:

- 上述のように、Touch ID搭載Magic KeyboardのPKAブロックとSecure Enclaveの安全なペアリング
- Touch IDセンサーを搭載したMagic KeyboardとそのPKAブロックの間の安全なチャネル

Touch IDセンサーを搭載したMagic KeyboardとそのPKAブロックの間の安全なチャネルは、両者で共有される一意の鍵を使用して工場で確立されます。（これは、Touch ID内蔵のMacコンピュータでMacのSecure Enclaveと内蔵センサーの間に安全なチャネルを作成するために使用されるものと同じテクニックです。）

Face ID、Touch ID、パスコード、パスワード

Face IDまたはTouch IDを使用するには、パスコードまたはパスワードでロック解除するようにユーザがデバイスを設定する必要があります。Face IDまたはTouch IDで認証に成功すると、デバイスのパスコードまたはパスワードを入力しなくてもユーザのデバイスの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やパスワ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またはパスワードもはるかに実用的なものとなります。Face IDやTouch IDは、ユーザのパスコードまたはパスワードに取って代わるものではありません。代わりに、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します。強力なパスコードまたはパスワードはユーザのiPhone、iPad、Mac、またはApple Watchによるそのユーザのデータの暗号化保護の基礎となるため、これは重要な点です。

デバイスのパスコードまたはパスワードが必要な場合

ユーザはいつでもFace IDやTouch IDの代わりにパスコードまたはパスワードを使用できますが、生体認証が禁止されている状況があります。セキュリティが重視される以下の操作では、常にパスコードまたはパスワードを入力する必要があります:

- 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
- 構成プロファイルのインストール
- Macの「システム設定」(macOS 13以降)の「プライバシーとセキュリティ」パネルのロック解除
- Macの「システム環境設定」(macOS 12以前)の「セキュリティとプライバシー」パネルのロック解除
- Macの「システム設定」(macOS 13以降)の「ユーザとグループ」パネルのロック解除(FileVaultがオンになっている場合)
- Macの「システム環境設定」(macOS 12以前)の「ユーザとグループ」パネルのロック解除(FileVaultがオンになっている場合)

デバイスが以下のいずれかの状態のときにもパスコードまたはパスワ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。
- ユーザがMacアカウントからログアウトした(またはまだログインしていない)場合。
- ユーザが48時間以上デバイスのロックを解除していない場合。
- ユーザが、156時間(6日半)、パスコードまたはパスワードを使用してデバイスのロックを解除しておらず、かつ4時間、生体認証を使用して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。
- ユーザが、いずれかの音量ボタンとスリープ/スリープ解除ボタンを2秒間同時に押したままにしてから「キャンセル」を押して、電源オフまたは緊急SOSを終了したとき。
- 生体認証に5回失敗したとき(ただし、利便性のために、数回失敗すると生体認証ではなくパスコードまたはパスワードの入力をすすめられる場合があります)。

iPhoneでマスクありのFace IDが有効になっている場合は、以下のいずれかのユーザアクションから6.5時間以内であれば利用できます:

- Face ID認証に成功(マスクありまたはマスクなし)
- デバイスパスコードによる検証
- Apple Watchによるデバイスのロック解除

これらのアクションのいずれかを行うと、実行後に6.5時間が延長されます。

iPhoneまたはiPadでFace IDまたはTouch IDが有効な場合、スリープ/スリープ解除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、Face IDまたはTouch IDで認証に成功するか、パスコードを使用する必要があります。

無作為に選ばれた他人がユーザのiPhoneまたはiPadのロックを解除できる確率は、Face IDの場合は100万分の1未満です(マスク着用時Face IDがオンになっている場合を含む)。ユーザのiPhone、iPad、MacがTouch IDを搭載している場合やMagic Keyboardとペアリングされている場合は、確率は5万分の1未満です。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、Face IDとTouch IDのどちらでも、認証に5回失敗したときはパスコードまたはパスワードを入力しなければユーザのデバイスまたはアカウントにアクセスできなくなります。Face IDでの誤認率は、以下の場合に高くなります:

- 双子やユーザによく似た兄弟姉妹
- 13歳未満の子供(この年齢層では顔の特徴がまだ十分に定まっていない場合があるため)

これら2つの場合の確率は、マスク着用時Face IDを使用している場合にはさらに高くなります。誤認率について懸念がある場合は、認証にパスコードを使用することをおすすめします。

顔照合のセキュリティ

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(赤外線)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。その後行われた調査には、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、さまざまな種類のサングラスなどを身に付けていても顔を認識できます。さらにFace IDは、iPhone 12以降のiPhoneデバイスおよびiOS 15.4以降では、マスクを着けた状態でのロック解除にも対応しています。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

通常の操作時にキャプチャされた顔の画像は保存されず、Face IDへの登録のため、または登録済みFace ID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。

Face IDの照合精度の向上

照合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。照合に成功したときは、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、特定回数の照合後に破棄されます。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照合後に破棄されます。Face IDをリセットするオプションが選択されたときにも、この新しいデータは破棄されます。こういった補強プロセスにより、Face IDはユーザの髪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。

Face IDとTouch IDの用途

デバイスまたはユーザアカウントのロック解除

Face IDまたはTouch IDがオフの場合は、デバイスまたはアカウント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またはパスワードを入力してデバイスまたはアカウントをロック解除しない限りアクセスできません。

Face IDまたはTouch IDがオンの場合は、デバイスまたはアカウント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Face IDまたはTouch IDサブシステムに与えられている鍵でラップされます。ユーザがデバイスまたはアカウント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、デバイスまたはアカウント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、Face IDまたはTouch 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、Face IDまたはTouch IDでデバイスまたはアカウントをロック解除するために必要な鍵は消去されます。また、パスコードまたはパスワードの入力が必要な状況になったときは、Secure Enclaveによってこれらの鍵が破棄されます。

Apple Payでの買い物のセキュリティ保護

ユーザは、Apple PayでFace IDとTouch IDを使って、店舗、アプリ、オンラインで簡単かつ安全に買い物をすることもできます:

- **店舗でFace IDを使用する:** 店舗での支払いをFace IDで認証する場合は、まず、ユーザが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。このダブルクリックにより、Secure Enclaveに直接リンクされる物理ジェスチャを使用したユーザの意思がキャプチャされ、悪質なプロセスによる偽造から保護します。次に、ユーザはFace IDで認証を行ってから、デバイスを非接触型決済リーダーに近付けます。Face IDで認証したあとに、Apple Payでの別の支払い方法を選択できます。この場合は認証をやり直す必要がありますが、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。
- **アプリ内またはWeb上でFace IDを使用する:** アプリ内またはオンラインで支払いをするときは、ユーザが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60秒以内にApple Pay決済が完了しなかった場合は、ユーザが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。
- **Touch IDを使用する:** Touch IDの場合、支払いの意思はTouch IDセンサーを有効にするジェスチャと、ユーザの指紋照合の成功を組み合わせて確認されます。

システムが提供するAPIを使用する

他社製アプリでは、システムが提供するAPIを使用して、Face ID、Touch ID、パスコード、またはパスワードによる認証をユーザに求めることができます。Touch IDをサポートするアプリでは、特別な変更なしにFace IDも自動的にサポートされます。Face IDまたはTouch IDの使用時は、アプリに認証の成否が通知されるだけで、アプリがFace ID、Touch 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。

キーチェーン項目の保護

キーチェーン項目をFace IDまたはTouch IDで保護して、認証成功、またはデバイスパスコードまたはアカウントパスワードでのみ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。アプリのデベロッパは、キーチェーン項目をロック解除するためにFace ID、Touch ID、パスコード、またはパスワードを要求する前に、ユーザによってパスコードまたはパスワ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。アプリデベロッパは以下のいずれかを行うことができます:

- 認証APIを使用する際にアプリ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アプリでは、ユーザが登録されているかどうかを確認した上で、Face IDまたはTouch IDを第2要素として使用できます。
- Secure Enclave内でECC(楕円曲線暗号)キーを生成して使用できます。これらはFace IDまたはTouch 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。

購入の実行と承認

ユーザはiTunes Store、App Store、Apple Booksなどでの購入の承認にFace IDまたはTouch IDを使用するように設定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。買い物をすると、Secure Enclaveにより生体認証が行われたことが確認されてから、店舗のリクエストに署名するのに使用されるECC鍵を解除します。

セキュアインテントとSecure Enclaveへの接続

セキュアインテントは、オペレーティングシステムまたはアプリケーションプロセッサとのやりとりなしでユーザの意図を確認する手段を提供します。この接続は物理的なボタンからSecure Enclaveへの物理リンクであり、以下のデバイスで使用できます:

- iPhone X以降
- Apple Watch Series 1以降
- iPad Pro(すべてのモデル)
- iPad Air(2020年)
- Appleシリコン搭載Macコンピュータ

ユーザはこのリンクにより、ルート権限またはカーネル内で実行されているソフトウェアであってもなりすましができないように設計された方法で、操作を実行する意図を確認できます。

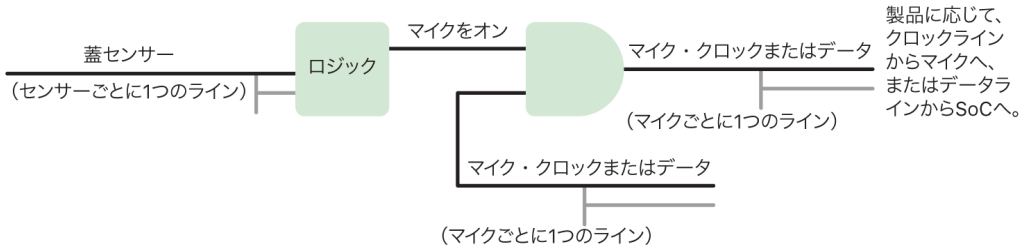
この機能は、Apple Payのトランザクションを行うときや、Touch ID搭載Magic KeyboardのAppleシリコン搭載Macへのペアリングを確定するときに、ユーザの意図を確認するために使用されます。ユーザインターフェイスによって指示されたときに該当するボタンを2回押す(Face IDの場合)か、指紋をスキャンする(Touch IDの場合)と、ユーザの意図が確認されたことになります。詳しくは、Apple Payでの買い物のセキュリティ保護を参照してください。Apple T2セキュリティチップを搭載し、Touch Barを搭載していないMacBookモデルでは、Secure EnclaveとT2ファームウェアに基づく同様の仕組みがサポートされます。

ハードウェアマイクの切断

AppleシリコンMacノートブックとIntelプロセッサおよびApple T2セキュリティチップ搭載Macノートブックはすべて、蓋が閉じられるたびにマイクを無効にするハードウェア切断機能を備えています。T2チップを搭載したすべての13インチMacBook ProおよびMacBook Airノートブック、2019以降のT2チップを搭載したすべてのMacBookノートブック、およびAppleシリコン搭載Macノートブックでは、この切断機能はハードウェアのみに実装されています。この切断機能は、macOSでルート権限またはカーネル権限を持つソフトウェアとT2チップなどのファームウェア上のソフトウェアも含め、どのソフトウェアも蓋が閉じられているときにはマイクを使用できないようにするためのものです。（カメラは、蓋が閉じられているときには視野が完全に覆い隠されるため、ハードウェアで切断されません。）

2020年以降のiPadのモデルもハードウェアマイク切断に対応しています。MFi準拠のケース（Appleで販売しているものなど）がiPadに装着され、閉じているときには、マイクがハードウェアで切断されます。これは、iPadOSでルート権限またはカーネル権限を持つソフトウェアとすべてのデバイスファームウェアも含め、どのソフトウェアもマイクのオーディオデータを使用できないようにするためです。

このセクションの保護はハードウェアロジックで直接実装されています。実装は次の回路図に従っています:



ハードウェアマイク切断機能がある各製品では、蓋やケースが物理的に閉じると、その作用の物理プロパティ（ホール効果センサーやヒンジ角度センサーなど）を使用して、蓋センサーがそれを検知します。較正が必要なセンサーでは、デバイスの生産中にパラメータが設定され、較正プロセス中にハードウェアが非可逆的にロックされ、その後センサーの重要パラメータはいかなる変更も不可能となります。これらのセンサーは、再プログラミング不可能なハードウェアロジックの単純なセットを通過する直接ハードウェア信号を放出します。このロジックにより、マイクを無効にする前に、デバウンス、ヒステリシス、最大500ミリ秒の遅延が提供されます。この信号を実装する方法は製品によって異なり、マイクとSystem on Chip（SoC）間でデータを通信するラインを無効にする方法と、マイクモジュールを有効にする入力ラインの1つ（例えばクロックラインなどの有効なコントロール）を無効にする方法があります。

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。

- 支払いカード、または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アクセスカード

サイドボタンを押すと、バッテリーアイコンが電力低下を示し、エクスプレスカードが使用可能であるというテキストが示されます。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、目に見える通知は表示されません。iPhone SE第2世代では、完了した決済が画面に表示されるまでに数秒かかります。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。

システムのセキュリティ

システムのセキュリティの概要

システムのセキュリティは、Apple製ハードウェアならではの高い性能を基盤として、使いやすさを損なわずにAppleデバイスのシステムリソースへのアクセスを制御します。システムのセキュリティの範囲は、ブートプロセス、ソフトウェアアップデート、およびCPU、メモリ、ディスク、ソフトウェアプログラム、保存データなどのコンピュータシステムリソースの保護におよびます。

Appleオペレーティングシステムの最新バージョンは最も安全です。Appleのセキュリティの重要な部分は、ブート時にシステムをマルウェア感染から保護する**セキュアブート**です。セキュアブートは、シリコンで始まります。そのあと、ソフトウェアを通じて信頼チェーンが構築されていきます。信頼チェーンの各段階は、その次の段階が適切に機能していることを確認した上で制御を引き渡すように設計されています。このセキュリティモデルは、Appleデバイスのデフォルトのブートだけでなく、Appleデバイスの復元や適切な時期のアップデートのさまざまなモードにも対応しています。Secure Enclaveなどのサブコンポーネントも、Appleによる既知の正常なコードのみをブートできるようにするために独自のセキュアブートを実行します。このアップデートシステムはダウングレード攻撃を防止するよう設計されています。デバイスを（攻撃者が侵入方法を知っている）古いバージョンのオペレーティングシステムにロールバックできなくなるので、ユーザデータを盗み出す手段が断たれます。

Appleのデバイスには起動とランタイムの保護機能もあり、操作の処理中に起動とランタイムの整合性が保持されます。iPhone、iPad、Appleシリコン搭載Mac、Apple Watch、Apple TV、およびHomePod上のAppleが設計したシリコンは、オペレーティングシステムの整合性を保護するための共通のアーキテクチャを備えています。また、macOSは、さまざまなコンピューティングモデルに対応する拡張された構成可能な保護機能のセット、およびすべてのMacハードウェアプラットフォームで対応する機能も備えています。

セキュアブート

iPhoneおよびiPadデバイスのブートプロセス

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、整合性チェックを有効にするためにAppleによって暗号化された署名が付いているため、ブートは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、カーネル拡張機能、モバイルデータ通信ネットワークの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は、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を検証するように設計されています。

iPhoneおよびiPad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と呼ばれる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ルート認証局（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、対象となるものが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またはiPadOS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あとに、iBootが読み込まれて検証されます。

以下の段階で読み込みまたは検証ができなかった場合、対象のハードウェアに応じて異なる処理が行われます:

- **Boot ROMでLLBを読み込めない（古いデバイス）:** デバイスファームウェアアップグレード（DFU）モード
- **LLBまたはiBoot:** リカバリモード

いずれの場合も、USB経由でデバイスをFinder（macOS 10.15以降）またはiTunes（macOS 10.14以前の場合）に接続し、工場出荷時のデフォルト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。このレジスタがアップデートされたあとに、以下のモードに入ります。

- **DFUモード:** Apple A12以降のSoCを搭載したデバイスでBoot ROMにより設定されます
- **リカバリモード:** Apple A10、S2、またはそれ以降のSoCを搭載したデバイスでiBootにより設定されます

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、モバイルデータ通信ネットワークのベースバンドサブシステムで、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追加のセキュアブートが実行されます。

Secure Enclaveでは、そのソフトウェアがAppleによって検証および署名されていることを確認するセキュアブートも実行されます。

メモリセーフなiBoot実装

iOS 14以降およびiPadOS 14以降では、セキュリティを向上させるために、iBootブートローダーのビルドに使用するCコンパイラツールチェーンを変更しました。変更されたツールチェーンは、通常はCプログラムで発生するメモリおよび型の安全性の問題を防止するように設計されたコードを実装します。例えば、以下のクラスでほとんどの脆弱性を防止します:

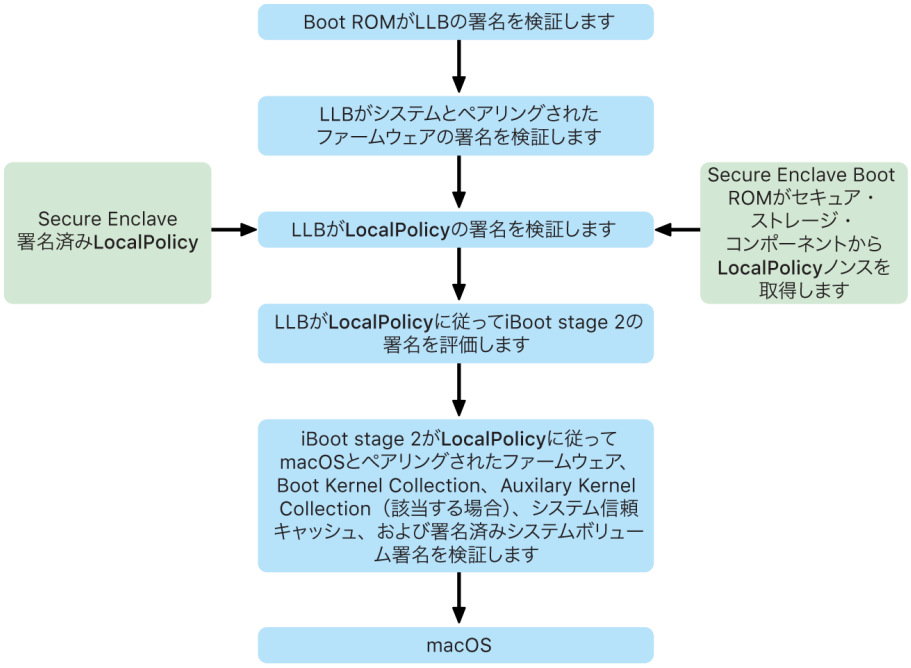
- バッファオーバーフロー。すべてのポインタがメモリにアクセスするときに検証される境界情報を渡すことを保証することによって防止
- ヒープの悪用。ヒープデータをそのメタデータから分離し、二重解放エラーなどのエラー状況を正確に検出することによって防止
- 型の取り違え。すべてのポインタがポインタキャスト演算中に検証されるランタイム型情報を渡すことを保証することによって防止
- 解放済みメモリの使用(use after free)エラーによって発生した型の取り違え。静的型によるすべての動的メモリ割り当てを分離することによって防止

このテクノロジーは、A13 Bionicチップ以降を搭載したiPhoneと、A14 Bionicチップ以降を搭載したiPadで使用できます。

Appleシリコン搭載Macコンピュータ

Appleシリコン搭載Macのブートプロセス

Appleシリコン搭載Macの電源を入れると、iPhoneやiPadのものと非常によく似たブートプロセスが実行されます。



このチップは信頼チェーンの最初のステップでBoot ROMからコードを実行します。Appleシリコン搭載Macでのmacosのセキュアブートは、オペレーティングシステムコード自体だけでなく、セキュリティポリシー、および承認されたユーザによって構成されたkext(サポートされていますが推奨されません)も検証します。

LLB（Low Level Bootloader）が起動すると、署名が検証され、ストレージ、ディスプレイ、システム管理、Thunderboltコントローラなどの SoC内コア用のシステムにペアリングされたファームウェアが読み込まれます。LLBは、Secure Enclaveプロセッサによって署名されたファイルであるLocalPolicyの読み込みも行います。LocalPolicyファイルは、ユーザがシステムのブートとランタイムのセキュリティポリシー用に選択した構成を記述したものです。LocalPolicyは他のすべてのブートオブジェクトと同じデータ構造形式ですが、ソフトウェアアップデートのように中央のAppleサーバによって署名されるのではなく、特定のコンピュータのSecure Enclave内でのみ使用できる秘密鍵によってローカルで署名されます。

以前のLocalPolicyのリプレイを防止するため、LLBではSecure Enclaveが接続されたセキュアストレージコンポーネントからアンチリプレイ値をルックアップする必要があります。そのためにSecure Enclave Boot ROMを使用し、LocalPolicyのアンチリプレイ値とセキュアストレージコンポーネントのアンチリプレイ値が一致することを確認します。これにより、低レベルのセキュリティ用に構成されていた可能性のある古いLocalPolicyが、セキュリティのアップグレード後にシステムに再適用されるのを防ぐことができます。その結果、Appleシリコン搭載Macでのセキュアブートでは、オペレーティングシステムのバージョンのロールバックだけでなく、セキュリティポリシーのダウングレードからも保護することができます。

LocalPolicyファイルは、オペレーティングシステムが「完全なセキュリティ」、「低セキュリティ」、「セキュリティ制限なし」のどれに合わせて構成されているかを取得します。

- **完全なセキュリティ:** システムはiOSやiPadOSのように動作し、インストール時に使用可能だった最新のものであることが分かっているソフトウェアのブートのみを許可します。
- **低セキュリティ:** LLBは、オペレーティングシステムにバンドルされている「グローバル」署名を信頼するよう指示されます。これにより、システムが古いバージョンのmacOSを実行することが許可されます。古いバージョンのmacOSには必ず、パッチが適用されていない脆弱性が含まれているため、このセキュリティモードは「**低セキュリティ**」と呼ばれます。これは、カーネル拡張機能（kext）のブートをサポートするために必要なポリシーレベルでもあります。
- **セキュリティ制限なし:** システムはiBoot以降のグローバル署名検証を使用するという点で「低セキュリティ」のように動作しますが、LocalPolicyの署名に使用されるのと同じ鍵でSecure Enclaveによって署名されている一部のブートオブジェクトを受け入れるべきであることもiBootに通知します。このポリシーレベルは、独自のカスタムXNUカーネルの構築、署名、およびブートを行うユーザをサポートします。

選択されたオペレーティングシステムが「完全なセキュリティ」で実行されていることをLocalPolicyがLLBに示している場合、LLBはiBoot用のパーソナライズされた署名を評価します。「低セキュリティ」または「セキュリティ制限なし」で実行されている場合は、グローバル署名を評価します。署名の検証エラーが発生すると、システムがrecoveryOSでブートして修復オプションが表示されます。

LLBがiBootに引き継ぐと、Secure Neural Engineや常時稼働プロセッサなどのファームウェアなど、macOSにペアリングされたファームウェアが読み込まれます。iBootは、LLBから渡されたLocalPolicyに関する情報も調べます。Auxiliary Kernel Collection（AuxKC）が存在すべきであることをLocalPolicyが示している場合、iBootはそれをファイルシステム上で探して、LocalPolicyと同じ鍵を使ってSecure Enclaveで署名されたことを検証し、そのハッシュがLocalPolicyに保存されているハッシュと一致することを検証します。AuxKCが検証されると、iBootは、ブートカーネルコレクションとAuxKCをカバーするメモリ領域全体をシステムコプロセッサ整合性保護（SCIP）でロックする前に、ブートカーネルコレクションを使用してメモリ内にAuxKCを配置します。ポリシーにAuxKCが存在する必要があることが示されていても、見つからない場合、システムはAuxKCなしでmacOSのブートを続けます。iBootが、署名済みシステムボリューム（SSV）のルートハッシュを検証して、カーネルがマウントするファイルシステムの整合性が完全に検証されることを確認します。

Appleシリコン搭載Macのブートモード

Appleシリコン搭載Macには、以下で説明するブートモードがあります。

モード	キーの組み合わせ	説明
macOS	シャットダウンの状態から、電源ボタンを押して**放します**。	1. Boot ROMがLLBに引き継ぎます。 2. LLBが、システムにペアリングされたファームウェアと選択したmacOSのLocalPolicyを読み込みます。 3. LLBが、macOSでブートしていることをブートプログレスレジスタ(BPR)にロックしてiBootに引き継ぎます。 4. iBootが、macOSにペアリングされたファームウェア、静的信頼キャッシュ、デバイスツリー、およびブートカーネルコレクションを読み込みます。 5. LocalPolicyが許可する場合は、iBootが他社製のkextのAuxKC(Auxiliary Kernel Collection)を読み込みます。 6. LocalPolicyが無効にしていなかった場合は、iBootが署名済みシステムボリューム(SSV)のルート署名ハッシュを検証します。
ペアリングされたrecoveryOS	シャットダウンの状態から、電源ボタンを**押したままにします**。	1. Boot ROMがLLBに引き継ぎます。 2. LLBが、システムにペアリングされたファームウェアとrecoveryOSのLocalPolicyを読み込みます。 3. LLBが、ペアリングされたrecoveryOSでブートしていることをブートプログレスレジスタにロックして、ペアリングされたrecoveryOS用のiBootに引き継ぎます。 4. iBootが、macOSにペアリングされたファームウェア、信頼キャッシュ、デバイスツリー、およびブートカーネルコレクションを読み込みます。 5. ペアリングされたrecoveryOSのブートが失敗すると、フォールバックrecoveryOSでのブートが試行されます。
フォールバックrecoveryOS	シャットダウンの状態から、電源ボタンを**2回押して押したままにします**。	1. Boot ROMがLLBに引き継ぎます。 2. LLBが、システムにペアリングされたファームウェアとrecoveryOSのLocalPolicyを読み込みます。 3. LLBが、ペアリングされたrecoveryOSでブートしていることをブートプログレスレジスタにロックして、recoveryOS用のiBootに引き継ぎます。 4. iBootが、macOSにペアリングされたファームウェア、信頼キャッシュ、デバイスツリー、およびブートカーネルコレクションを読み込みます。
セーフモード	上記のようにrecoveryOSでブートしてから、**Shiftキー**を押しながら起動ボリュームを選択します。	1. 上記のようにrecoveryOSで起動します。 2. Shiftキーを押しながらボリュームを選択すると、BootPickerアプリは通常通りそのmacOSのブートを承認し、次回のブート時にAuxKCを読み込まないようにiBootに指示する`nvram`変数も設定します。 3. システムが再起動し、対象のボリュームでブートされますが、iBootでAuxKCは読み込まれません。

ペアリングされたrecoveryOSの制限

macOS 12.0.1以降では、新しいmacOSをインストールすると、ペアリングされたバージョンのrecoveryOSも対応するAPFSボリュームグループに必ずインストールされます。この設計はIntelプロセッサ搭載Macコンピュータのユーザには馴染みあるものですが、Appleシリコン搭載Macでは、これによってセキュリティおよび互換性の保証が強化されます。macOSのインストールに専用のrecoveryOSがペアリングされるようになるため、そのペアリングされたrecoveryOSのみがセキュリティをダウングレードする操作を実行できることを保証するのに役立ちます。これは、新しいバージョンのmacOSのインストールの改ざんが古いバージョンのmacOSから開始されること、およびその逆の改ざんから保護するのに役立ちます。

ペアリングの制限は以下のように適用されます:

- macOS 11のすべてのインストールはrecoveryOSにペアリングされます。macOS 11のインストールがデフォルトでブートするよう選択されている場合、Appleシリコン搭載Macではブート時に電源キーを押したままにすることでrecoveryOSがブートします。recoveryOSは任意のmacOS 11インストールのセキュリティ設定をダウングレードできますが、macOS 12.0.1のインストールをダウングレードすることはできません。
- macOS 12.0.1以降のインストールがデフォルトでブートするよう選択されている場合、Macの起動時に電源キーを押したままにすることでペアリングされたrecoveryOSがブートします。ペアリングされたrecoveryOSはペアリングされたmacOSインストールのセキュリティ設定をダウングレードできますが、その他のmacOSインストールをダウングレードすることはできません。

任意のmacOSインストールのペアリングされたrecoveryOSをブートするには、そのインストールがデフォルトとして選択されている必要があります。これは、「システム設定」の「一般」>「起動ディスク」(macOS 13以降)または「システム環境設定」の「起動ディスク」(macOS 12以前)を使用するか、recoveryOSを起動して、Optionキーを押したままボリュームを選択することで行います。

注記: フォールバックrecoveryOSは、任意のmacOSインストールのダウングレードを実行できません。

Appleシリコン搭載Macの起動ディスクのセキュリティポリシー管理

概要

Intelプロセッサ搭載Macのセキュリティポリシーとは異なり、Appleシリコン搭載Macのセキュリティポリシーは、インストールされているオペレーティングシステムごとに適用されます。これは、バージョンとセキュリティポリシーが異なる複数のインストール済みmacOSインスタンスが同じMacでサポートされることを意味します。この理由から、起動セキュリティユーティリティに**オペレーティングシステムピッカー**が追加されました。

Appleシリコン搭載Macでは、システムセキュリティユーティリティが、kextのブートやシステム整合性保護(SIP)の構成など、ユーザが構成したmacOSの全体的なセキュリティ状態を示します。セキュリティ設定の変更によりセキュリティが大幅に低下したりシステム侵害が生じやすくなったりする場合、変更を行うためには、ユーザが電源ボタンを押したままにしてrecoveryOSに入る必要があります(マルウェアは信号をトリガできず、物理的にアクセスできる人間のみがトリガできます)。このため、Appleシリコン搭載Macもファームウェアパスワードを必要としません(またはサポートしません)。すべての重要な変更は、ユーザ承認によってすでに制御されています。SIPについて詳しくは、システム整合性保護を参照してください。

「完全なセキュリティ」と「低セキュリティ」は、recoveryOSから起動セキュリティユーティリティを使用して設定できます。ただし、「セキュリティ制限なし」には、Macの安全性が大幅に低下するリスクを受け入れるユーザが、コマンドラインツールからのみアクセスできます。

「完全なセキュリティ」のポリシー

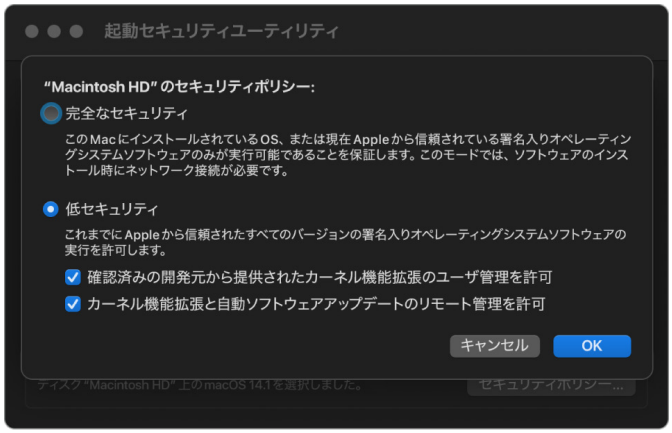
「完全なセキュリティ」はデフォルトの設定であり、iOSおよびiPadOSと同様に動作します。macOSでは、ソフトウェアがダウンロードされ、インストールの準備が完了した時点で、ソフトウェアに付属するグローバル署名を使用するのではなく、iOSおよびiPadOSで使用されるものと同じAppleの署名サーバと通信して、新しい「パーソナライズされた」署名を要求します。署名は、署名リクエストの一部としてECID（Exclusive Chip Identification）（この場合はApple CPUごとに固有のID）が含まれているときにパーソナライズされます。署名サーバから送り返される署名は一意になり、署名を要求したApple CPUのみで使用できます。「完全なセキュリティ」のポリシーが有効な場合、提供された署名がAppleによるものということだけでなく、そのMacのみのために署名されていて、実質的にそのバージョンのmacOSをそのMacに関連付けるものであることがBoot ROMとLLBによって保証されます。

オンラインの署名サーバを利用すると、一般的なグローバル署名方式に比べ、ロールバック攻撃からの保護も強化されます。グローバル署名システムでは、セキュリティエポックが何回もロールされている可能性がありますが、最新のファームウェアが実装されたことがないシステムではそのことが認識されません。例えば、現在自らのセキュリティエポックが1であると認識しているコンピュータは、現在の実際のセキュリティエポックが5であっても、セキュリティエポック2のソフトウェアを受け入れてしまいます。Appleシリコンのオンライン署名システムでは、セキュリティエポックが最新でないソフトウェア用の署名の作成を署名サーバが拒否できます。

また、攻撃者がセキュリティエポックの変化後に脆弱性を発見しても、以前のエポックに属する脆弱なソフトウェアをシステムAから選んで、攻撃のためにシステムBに適用することはできません。エポックの古い脆弱なソフトウェアがシステムA用にパーソナライズされていたことにより、その脆弱なソフトウェアを転送できないため、それがシステムBの攻撃に使用されることはありません。これらすべてのメカニズムが連携するため、最新のソフトウェアによる保護を回避するために攻撃者がMacに脆弱なソフトウェアを意図的に配置することが不可能であることがより強固に保証されます。ただし、Macの管理者ユーザ名とパスワードを所有しているユーザは、自らのユースケースに最適なセキュリティポリシーをいつでも選択できます。

「低セキュリティ」のポリシー

「低セキュリティ」は、T2チップとIntelプロセッサを搭載したMacでの「中程度のセキュリティ」の動作に似ていて、ベンダー（この場合は、Apple）はコードが自身によって提供されたものであることを保証するために、コードのデジタル署名を生成します。この設計により、攻撃者が無署名のコードを挿入することを阻止できます。Appleではこの署名を「グローバル」署名と呼びます。この署名は現在「低セキュリティ」のポリシーが設定されているMacで任意の期間使用できるからです。不正なオペレーティングシステムの変更によりユーザデータにアクセスできなくなる可能性がありますが、「低セキュリティ」自体はロールバック攻撃に対する保護を提供しません。詳しくは、Appleシリコン搭載Macのカーネル拡張機能を参照してください。

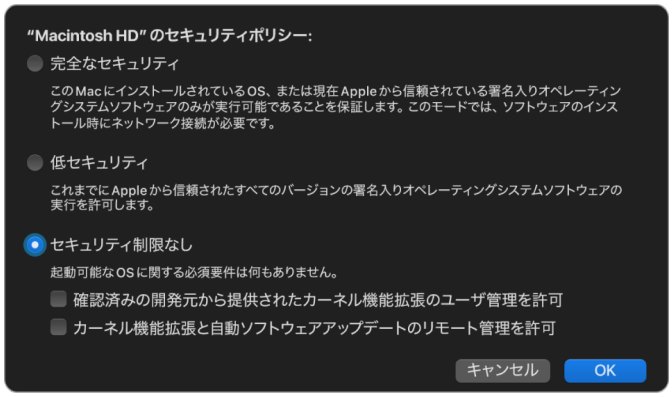


「低セキュリティ」は、ユーザが古いバージョンのmacOSを実行できるようにするだけでなく、他社製のカーネル拡張機能（kext）の導入など、ユーザのシステムセキュリティを危険にさらす可能性のあるその他のアクションにも必要です。kextはカーネルと同じ権限を持っているため、他社製のkextに脆弱性があると、オペレーティングシステム全体が侵害される可能性があります。このような理由で、デベロッパには、将来のAppleシリコン搭載MacコンピュータのmacOSからkextサポートが削除される前に、システム機能拡張を採用することが強く推奨されています。他社製のkextは、有効になっている場合でも、カーネル内にオンデマンドで読み込むことはできません。その代わりに、それらのkextは、LocalPolicyにハッシュが保存されているAuxiliary Kernel Collection（AuxKC）に結合され、その結果として再起動が要求されます。AuxKCの生成について詳しくは、macOSのカーネルの安全な拡張を参照してください。

「セキュリティ制限なし」のポリシー

「セキュリティ制限なし」は、Macをはるかに安全でない状態にするリスクを受け入れるユーザ向けです。このモードは、T2チップとIntelプロセッサを搭載したMacの「セキュリティなし」モードとは異なります。「セキュリティ制限なし」では、署名の検証は引き続きセキュアブートチェーン全体で実行されますが、ポリシーを「制限なし」に設定すると、カスタムXNUカーネルから構築されたユーザ生成ブートカーネルコレクションのような、Secure Enclaveで署名されたブートオブジェクトをローカルで受け入れるべきであることがiBootに伝達されます。この方法により、「セキュリティ制限なし」でも、任意の「完全に信頼されていないオペレーティングシステム」カーネルを実行するためのアーキテクチャ機能が備わります。カスタムのブートカーネルコレクションまたは完全には信頼されていないオペレーティングシステムがシステムに読み込まれると、一部の復号鍵が使用できなくなります。これは、完全には信頼されていないオペレーティングシステムが信頼できるオペレーティングシステムのデータにアクセスできないようにするためです。

重要: AppleはカスタムXNUカーネルを提供またはサポートしていません。



「セキュリティ制限なし」がT2チップとIntelプロセッサを搭載したMacの「セキュリティなし」とは異なる点がもう1つあります。これは、過去に独立して制御可能であった一部のセキュリティダウングレードの前提条件です。特に、Appleシリコン搭載MacでシステムIntegrity Protection(SIP)を無効にするには、ユーザはシステムを「セキュリティ制限なし」に設定していることを確認する必要があります。SIPを無効にすると常に、カーネルがはるかに容易に侵害されるような状態にシステムが置かれるためです。特に、AppleシリコンMacでSIPを無効にすると、AuxKCの生成時にkext署名の適用が無効になり、任意のkextをカーネルメモリに読み込むことが許可されます。Appleシリコン搭載Macで行われたSIPのもう1つの改善点は、ポリシーストアがNVRAMからLocalPolicyに移動されたことです。そのため、SIPを無効にするには、電源ボタンを押したままにしてアクセスしたrecoveryOSから、LocalPolicy署名鍵にアクセスできるユーザによる認証が必要です。これにより、ソフトウェアのみの攻撃者だけでなく、Macに物理的にアクセスできる攻撃者にとっても、SIP無効化の難易度が大幅に高まります。

起動セキュリティユーティリティアプリから「セキュリティ制限なし」にダウングレードすることはできません。ユーザは、`csrutil`(SIPを無効にする)など、recoveryOSのターミナルからコマンドラインツールを実行することによってのみダウングレードできます。ユーザがダウングレードしたあと、それが発生したという事実が起動セキュリティユーティリティに反映されるため、ユーザはセキュリティをより安全なモードに簡単に設定できます。

注記: 技術的にはすべてのブートがローカルで実行されるため、Appleシリコン搭載Macは特定のメディアのブートポリシーを必要とせず、サポートしません。ユーザが外部メディアからのブートを選択する場合は、recoveryOSからの認証済み再起動を用いて、まずそのオペレーティングシステムバージョンをパーソナライズする必要があります。この再起動によって、外部メディアに保存されたオペレーティングシステムから信頼できるブートを実行するために使用される、LocalPolicyファイルが内部ドライブに作成されます。これは、外部メディアからの起動の設定は常に、オペレーティングシステムごとに明示的に有効にされ、すでにユーザの承認が要求されているという意味で、追加のセキュリティ設定は必要ありません。

LocalPolicyの署名キーの作成と管理

作成

macOSが工場で初めてインストールされたとき、またはテザリングされた消去インストールが実行されたときに、Macは一時的な復元用RAMディスクからコードを実行してデフォルト状態を初期化します。このプロセス中に、復元環境で、Secure Enclaveに保持される公開鍵と秘密鍵の新しいペアが作成されます。秘密鍵は、**所有者ID鍵(OIK)**と呼ばれます。OIKがすでに存在する場合は、このプロセスの一環として破棄されます。復元環境では、アクティベーションロックに使用される鍵である**ユーザID鍵(UIK)**も初期化されます。Appleシリコン搭載Macに固有のこのプロセスの一部として、アクティベーションロックのUIK認証が要求されたときに、検証時にLocalPolicyに適用される一連の要求された制約が組み込まれます。デバイスがアクティベーションロック用に認証されたUIKを取得できない場合(例えば、デバイスが現時点で「Macを探す」アカウントに関連付けられており、紛失したと報告されているために)、LocalPolicyの作成に進むことはできません。デバイスに**ユーザID証明書(ucrt)**が発行されている場合、そのucrtには、X.509 v3拡張内のサーバが課したポリシー制約とユーザが要求したポリシー制約が含まれます。

アクティベーションロック`ucrt`が正常に取得されると、サーバ側のデータベースに保存され、デバイスにも返されます。デバイスにucrtが設定されると、OIKに対応する公開鍵の認証要求が**基本アテステーション機関(BAA)**サーバに送信されます。BAAは、BAAがアクセス可能なデータベースに格納されているucrtからの公開鍵を使用して、OIK認証要求を検証します。認証を検証できた場合、BAAは公開鍵を認証し、BAAによって署名されていてucrtに格納されている制約が含まれている**所有者ID証明書(OIC)**を返します。OICはSecure Enclaveに送り返されます。それ以降、Secure Enclaveが新しいLocalPolicyに署名するたびに、OICがImage4に添付されます。LLBにはBAAルート証明書への信頼が組み込まれているため、OICが信頼され、LocalPolicy署名全体が信頼されます。

RemotePolicyの制約

LocalPolicyだけでなく、すべてのImage4ファイルには、Image4マニフェスト評価に関する制約が含まれています。これらの制約は、リーフ証明書の特殊なオブジェクト識別子(OID)を使用してエンコードされています。Image4検証ライブラリは、署名の評価中に証明書から特別な証明書制約OIDをルックアップし、そこに規定されている制約を機械的に評価します。制約の形式は次の通りです:

- Xが存在しなければならない
- Xが存在してはならない
- Xには特定の値が含まれていなければならない

そのため、例えば「パーソナライズされた」署名の場合、証明書の制約には「ECIDが存在しなければならない」が含まれ、「グローバル」署名の場合は「ECIDが存在してはならない」が含まれます。これらの制約は、誤って署名されたImage4マニフェストの生成を回避するために、特定の鍵で署名されたすべてのImage4ファイルが特定の要件に準拠することを必須にするためのものです。

各LocalPolicyのコンテキストでは、これらのImage4証明書の制約は**RemotePolicy**と呼ばれます。ブート環境のLocalPolicyごとに異なるRemotePolicyが存在できます。RemotePolicyは、recoveryOS LocalPolicyを制限するために使用されるため、recoveryOSのブート時に「完全なセキュリティ」でブートしているようにしか動作できません。これにより、ポリシーを変更できる場所としてのrecoveryOSブート環境の整合性に対する信頼が高まります。RemotePolicyは、LocalPolicyが生成されたMacのECIDと、そのMacのセキュアストレージコンポーネントに保存されているRemotePolicyノンスハッシュ(`rpnh`)が含まれるようにLocalPolicyを制限します。`rpnh`は(したがってRemotePolicyも)、「Macを探す」およびアクティベーションロックで登録、登録解除、リモートロック、リモートワイプなどのアクションが実行されたときにのみ変更されます。RemotePolicyの制約は、ユーザID鍵(UIK)の認証時に決定および指定され、発行済みユーザID証明書(ucrt)に署名されます。ECID、ChipID、BoardIDなどの一部のRemotePolicyの制約は、サーバによって決定されます。これは、あるデバイスが別のデバイスのLocalPolicyファイルに署名するのを防ぐためです。ほかのRemotePolicyの制約は、現在のOIKにアクセスするために必要なローカル認証とデバイスがアクティベーションロックされているアカウントのリモート認証の両方を提供せずにLocalPolicyのセキュリティがダウングレードするのを防ぐために、デバイスによって指定される場合があります。

Appleシリコン搭載MacのLocalPolicyファイルの内容

LocalPolicyはSecure Enclaveで署名されたImage4ファイルです。Image4は、ASN.1(Abstract Syntax Notation One)DERでエンコードされたデータ構造形式であり、Appleプラットフォーム上のセキュアブートチェーンオブジェクトに関する情報を記述するために使用されます。Image4ベースのセキュアブートモデルでは、セキュリティポリシーは、中央のApple署名サーバへの署名リクエストによって開始されたソフトウェアインストール時に要求されます。ポリシーが受け入れ可能だった場合、署名サーバは、さまざまな4文字コード(4CC)のシーケンスを含む署名済みのImage4ファイルを返します。これらの署名済みのImage4ファイルと4CCは、起動時にBoot ROMやLLBなどのソフトウェアによって評価されます。

オペレーティングシステム間の所有権の引き渡し

所有者ID鍵(OIK)へのアクセスは、「所有権」と呼ばれます。ポリシーまたはソフトウェアの変更を行ったあと、ユーザがLocalPolicyに再署名できるようにするには、所有権が必要です。OIKは、シールドキー保護(SKP)で説明されているのと同じ鍵階層で保護され、ボリューム暗号鍵(VEK)と同じキー暗号鍵(KEK)で保護されます。これは、通常、ユーザパスワードと、オペレーティングシステムおよびポリシーの測定値の両方によって保護されていることを意味します。Macのすべてのオペレーティングシステムに対応するOIKは1つだけです。そのため、2つ目のオペレーティングシステムをインストールする場合、2つ目のオペレーティングシステムのユーザに所有権を引き渡すには、最初のオペレーティングシステムのユーザからの明示的な同意が必要です。ただし、インストーラが1つ目のオペレーティングシステムから実行されている時点では、2つ目のオペレーティングシステムのユーザはまだ存在していません。オペレーティングシステムのユーザは通常、オペレーティングシステムがブートして設定アシスタントが実行されるまで生成されません。そのため、Appleシリコン搭載Macに2つ目のオペレーティングシステムをインストールする際は、次の2つの新しいアクションが必要です:

- 2つ目のオペレーティングシステム用のLocalPolicyを作成する
- 所有権を引き渡すために「インストールユーザ」を準備する

インストールアシスタントを実行していて、空のセカンダリーボリューム用のインストールを目的としている場合は、2つ目のボリュームの最初のユーザにするユーザを現在のボリュームからコピーするかどうかを確認するプロンプトが表示されます。ユーザが「はい」と答えた場合、作成される「インストールユーザ」は、実際には選択されたユーザのパスワードとハードウェア鍵から導出されたKEKであり、そのあと2つ目のオペレーティングシステムに渡されるときにOIKを暗号化するために使用されます。そのあと、新しいオペレーティングシステムのSecure EnclaveのOIKにアクセスできるようにするため、2つ目のオペレーティングシステムのインストールアシスタント内から、そのユーザのパスワードの入力が求められます。ユーザがユーザをコピーしないことを選択した場合でも、インストールユーザは同じ方法で作成されますが、ユーザのパスワードではなく空のパスワードが使用されます。この2番目のフローは、特定のシステム管理シナリオ用に存在します。ただし、マルチボリュームインストール構成にして、最も安全な方法で所有権の引き渡しを実行したい場合は、必ず、1つ目のオペレーティングシステムから2つ目のオペレーティングシステムにユーザをコピーする手順を選択する必要があります。

Appleシリコン搭載MacのLocalPolicy

Appleシリコン搭載Macの場合、ローカルのセキュリティポリシー管理は、Secure Enclaveで実行されているアプリケーションに委任されています。このソフトウェアは、ユーザの資格情報とプライマリCPUのブートモードを利用して、だれがどのブート環境からセキュリティポリシーを変更できるかを決定できます。これにより、悪質なソフトウェアがダウングレードしてより多くの特権を取得することによって、ユーザに対するセキュリティポリシー管理を使用するのを防ぐことができます。

LocalPolicyのマニフェストのプロパティ

LocalPolicyファイルには、ボードまたはモデルID（BORD）、特定のAppleチップ（CHIP）の指定、Exclusive Chip Identification（ECID）など、ほとんどすべてのImage4ファイルで見つかるアーキテクチャ4CCが含まれています。ただし、以下の4CCではユーザが構成できるセキュリティに絞って説明します。

注記: Appleは**ペアリングされたOne True recoveryOS（1TR）**という用語を使用して、物理的な電源ボタンを1回押したままにしてペアリングされたrecoveryOSがブートすることを示しています。これは、通常のrecoveryOSブート（NVRAMを使用してまたは2回押したままにして発生する、または起動時にエラーが発生したときに発生する可能性がある）とは異なります。特定の方法で物理的にボタンを押すことで、macOSに侵入したソフトウェアのみの攻撃者がそのブート環境に到達できないという信頼性が高まります。

LocalPolicyのノンスハッシュ（lpnh）

- **型:** OctetString (48)
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** `lpnh`はLocalPolicyのリプレイ防止に使用されます。これは、セキュアストレージコンポーネントに格納されているLocalPolicyノンス（LPN）のSHA384ハッシュで、Secure Enclave Boot ROMまたはSecure Enclaveを使用してアクセスできます。生のアンチリプレイ値はアプリケーションプロセッサからは見えず、sepOSのみから見ることができます。以前にキャプチャしたことのあるLocalPolicyが有効であることをLLBに確信させたい攻撃者は、リプレイしたいLocalPolicyで見つかったものと同じ`lpnh`値にハッシュする値をセキュアストレージコンポーネントに配置する必要があります。通常、システム上で有効なLPNは1つですが、ソフトウェアのアップデート中は2つが同時に有効であるため、アップデートエラーが発生した場合に古いソフトウェアのブートにフォールバックする可能性があります。オペレーティングシステムのLocalPolicyが変更されると、すべてのポリシーは、セキュアストレージコンポーネントにある新しいLPNに対応する新しい**lpnh**値で再署名されます。この変更は、ユーザがセキュリティ設定を変更するか、それぞれ新しいLocalPolicyを使用する新しいオペレーティングシステムを作成したときに行われます。

リモートポリシーのノンスハッシュ（rpnh）

- **型:** OctetString (48)
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** `rpnh`は`lpnh`と同じように動作しますが、「探す」の登録の状態の変更時など、リモートポリシーがアップデートされたときにのみアップデートされます。この変更は、ユーザがMacの「探す」の状態を変更したときに行われます。

recoveryOSのノンスハッシュ（ronh）

- **型:** OctetString (48)
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** `ronh`はlpnhと同じように動作しますが、システムrecoveryOSのLocalPolicyでのみ見つかります。ソフトウェアのアップデート時など、システムrecoveryOSがアップデートされたときにアップデートされます。`lpnh`および`rpnh`とは別のアンチリプレイ値が使用されるため、「探す」によってデバイスが無効な状態になったときに、システムrecoveryOSをブート可能にしたまま、LPNおよびRPNをセキュアストレージコンポーネントから削除することにより、既存のオペレーティングシステムを無効にすることができます。このようにして、システム所有者が「探す」アカウントに使用されるiCloudパスワードを入力することによってシステムに対する制御を証明したときに、オペレーティングシステムを再度有効にすることができます。この変更は、ユーザがシステムrecoveryOSをアップデートしたか、新しいオペレーティングシステムを作成したときに行われます。

次ステージImage4マニフェストハッシュ(nsih)

- **型:** OctetString (48)
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** **nsih**フィールドは、ブートされたmacOSを記述するImage4マニフェストデータ構造のSHA384ハッシュを表します。macOSのImage4マニフェストには、iBoot、静的信頼キャッシュ、デバイスツリー、ブートカーネルコレクション、署名済みシステムボリューム(SSV)のボリュームルートハッシュなどのすべてのブートオブジェクトの測定値が含まれています。LLBは、特定のmacOSをブートするように指示されている場合、iBootに添付されたmacOS Image4マニフェストのハッシュが、LocalPolicyの`nsih`フィールドでキャプチャされたものと一致することを保証するように設計されています。このようにして、`nsih`は、ユーザがLocalPolicyを作成したオペレーティングシステムのユーザの意図をキャプチャします。ユーザは、ソフトウェアのアップデートを実行するときに、暗黙的に`nsih`値を変更します。

Cryptex1 Image4マニフェストハッシュ(spih)

- **型:** OctetString (48)
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** `spih`フィールドは、Cryptex1 Image4マニフェストデータ構造のSHA384ハッシュを表します。Cryptex1 Image4マニフェストには、そのcryptexの測定値、ファイルシステムシール、関連する信頼キャッシュが含まれています。macOSの起動中にXNUカーネルとページ保護レイヤーによって、Cryptex1 Image4マニフェストハッシュが、iBootがLocalPolicyの`spih`フィールドから公開した内容と一致することが確認されます。ユーザは、緊急セキュリティ対応をインストールするかソフトウェアアップデートを実行する際に`spih`値を暗黙的に変更することになります。Cryptex1 Image4マニフェストハッシュは、次ステージImage4マニフェストハッシュとは無関係にアップデートできます。

Cryptex1生成(stng)

- **型:** 64ビットの符号なし整数
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** `stng`フィールドは、LocalPolicyでCryptex1 Image4マニフェストハッシュが最後にいつアップデートされたかを表すカウンタ値で、受信Cryptexを適用するためにページ保護レイヤーがローカルポリシーを評価しているときに、`lpnh`の代わりにアンチリプレイ値を提供します。ユーザは、緊急セキュリティ対応またはソフトウェアアップデートをインストールする際に`stng`値を暗黙的に増やすことになります。

AuxKC(Auxiliary Kernel Collection)ポリシーのハッシュ(auxp)

- **型:** OctetString (48)
- **変更可能な環境:** macOS
- **説明:** `auxp`は、ユーザが承認したkextリスト(UAKL)ポリシーのSHA384ハッシュです。これは、ユーザが承認したkextのみがAuxKCに含まれることを保証するために、AuxKCの生成時に使用されます。`smb2`はこのフィールドを設定するための前提条件です。ユーザは、「システム設定」の「プライバシーとセキュリティ」(macOS 13以降)または「システム環境設定」の「セキュリティとプライバシー」パネル(macOS 12以前)からkextを承認してUAKLを変更する際に、`auxp`値を暗黙的に変更することになります。

AuxKC（Auxiliary Kernel Collection）のImage4マニフェストのハッシュ（auxi）

- **型:** OctetString (48)
- **変更可能な環境:** macOS
- **説明:** システムは、UAKLハッシュがLocalPolicyの`auxp`フィールドで見つかるものと一致することを検証したあと、AuxKCがLocalPolicy署名を担当するSecure Enclaveプロセッサアプリケーションによって署名されることを要求します。次に、以前に署名されたAuxKCが複数混在していて、ブート時にそれらがオペレーティングシステムと照合される可能性を回避するため、AuxKC Image4マニフェスト署名のSHA384ハッシュがLocalPolicyに配置されます。iBootは、LocalPolicyで`auxi`フィールドを見つけると、ストレージからAuxKCを読み込んで、その署名を検証しようとします。また、AuxKCに添付されたImage4マニフェストのハッシュが、`auxi`フィールドで見つかった値と一致することも検証します。何らかの理由でAuxKCの読み込みに失敗した場合、システムはこのブートオブジェクトなしで、したがって他社製のkextを読み込まずに、ブートを続行します。`auxp`フィールドは、LocalPolicyのauxiフィールドを設定する場合の前提条件です。ユーザは、「システム設定」の「プライバシーとセキュリティ」（macOS 13以降）または「システム環境設定」の「セキュリティとプライバシー」パネル（macOS 12以前）からkextを承認してUAKLを変更する際に、`auxi`値を暗黙的に変更することになります。

AuxKC（Auxiliary Kernel Collection）受信確認ハッシュ（auxr）

- **型:** OctetString (48)
- **変更可能な環境:** macOS
- **説明:** `auxr`はAuxKC受信確認のSHA384ハッシュであり、AuxKCに含まれていたkextの正確なセットを示します。kextは、攻撃に使用されることが分かっている場合は、ユーザが承認したものであってもAuxKCから除外できるため、AuxKC受信確認はUAKLのサブセットでもかまいません。さらに、ユーザとカーネルの境界を破るために使用できる一部のkextは、Apple Payを使用できなかったり4KおよびHDRコンテンツを再生できなかったりといった機能の低下につながる可能性があります。これらの機能を希望するユーザは、より制限の厳しいAuxKCを含めることを選択します。`auxp`フィールドは、LocalPolicyの`auxr`フィールドを設定する場合の前提条件です。ユーザは、「システム設定」の「プライバシーとセキュリティ」（macOS 13以降）または「システム環境設定」の「セキュリティとプライバシー」パネル（macOS 12以前）から新しいAuxKCを構築する際に、`auxr`値を暗黙的に変更することになります。

CustomOS Image4マニフェストハッシュ（coih）

- **型:** OctetString (48)
- **変更可能な環境:** 1TR
- **説明:** `coih`はCustomOS Image4マニフェストのSHA384ハッシュです。iBootは、制御を移すためにXNUカーネルではなくそのマニフェストのペイロードを使用します。ユーザは、1TRで`kmutil configure-boot`コマンドラインツールを使用するときに、暗黙的に`coih`の値を変更します。

APFSボリュームグループUUID（vuid）

- **型:** OctetString (16)
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** `vuid`は、カーネルがルートとして使用すべきボリュームグループを示します。このフィールドは主に情報提供用でありセキュリティの制約には使用されません。この`vuid`は、新しいオペレーティングシステムインストールの作成時にユーザによって暗黙的に設定されます。

キー暗号鍵(KEK)グループUUID(kuid)

- **型:** OctetString (16)
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** `kuid`は、ブートされたボリュームを示します。キー暗号鍵は、通常はデータ保護のために使用されています。LocalPolicyごとに、LocalPolicy署名鍵を保護するために使用されます。この`kuid`は、新しいオペレーティングシステムインストールの作成時にユーザによって暗黙的に設定されます。

ペアリングされたrecoveryOS Trusted Boot Policy Measurement(prot)

- **型:** OctetString (48)
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** ペアリングされたrecoveryOSのTrusted Boot Policy Measurement(TBPM)は、アンチリプレイ値を除く、LocalPolicyのImage4マニフェストに対する特殊な反復SHA384ハッシュ計算で、経時的に一貫した測定値を出力する目的で実行されます(`lpnh`のようなアンチリプレイ値は頻繁にアップデートされるため)。`prot`フィールドは各macOS LocalPolicyにのみ見つかり、macOS LocalPolicyに対応するrecoveryOS LocalPolicyを示すペアリングを提供します。

Secure Enclaveで署名済みかどうかを示すrecoveryOSローカルポリシー(hrlp)

- **型:** ブール値
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** `hrlp`は、`prot`値(上記)が、Secure Enclaveで署名されたrecoveryOS LocalPolicyの測定値かどうかを示します。そうでない場合、recoveryOSのLocalPolicyは、macOSのImage4ファイルなどに署名するAppleオンライン署名サーバによって署名されます。

ローカルオペレーティングシステムのバージョン(love)

- **型:** ブール値
- **変更可能な環境:** 1TR、recoveryOS、macOS
- **説明:** `love`はLocalPolicyが作成されるOSバージョンを示します。バージョンは、LocalPolicy作成中に次の状態のマニフェストから取得され、recoveryOSのペアリング制限を適用するために使用されます。

安全なマルチブート(smb0)

- **型:** ブール値
- **変更可能な環境:** 1TR、recoveryOS
- **説明:** `smb0`が存在していてtrueの場合は、LLBは、パーソナライズされた署名を要求する代わりに、次ステージImage4マニフェストがグローバルに署名されることを許可します。ユーザはこのフィールドを、起動セキュリティユーティリティまたは`bputil`を使用して「低セキュリティ」にダウングレードすることで変更できます。

安全なマルチブート(smb1)

- **型:** ブール値
- **変更可能な環境:** 1TR
- **説明:** `smb1`が存在していてtrueの場合は、iBootは、カスタムのカーネルコレクションなどのオブジェクトがLocalPolicyと同じ鍵でSecure Enclaveで署名されることを許可します。`smb0`の指定は、`smb1`の指定の前提条件です。ユーザはこのフィールドを、`csrutil`や`bputil`などのコマンドラインツールを使用して「セキュリティ制限なし」にダウングレードすることで変更できます。

安全なマルチブート(smb2)

- **型:** ブール値
- **変更可能な環境:** 1TR
- **説明:** `smb2`が存在していてtrueの場合は、iBootは、Auxiliary Kernel CollectionがLocalPolicyと同じ鍵でSecure Enclaveで署名されることを許可します。`smb0`の指定は、`smb2`の指定の前提条件です。ユーザはこのフィールドを、起動セキュリティユーティリティまたは`bputil`を使用して、「低セキュリティ」にダウングレードして他社製のkextを有効にすることで変更できます。

安全なマルチブート(smb3)

- **型:** ブール値
- **変更可能な環境:** 1TR
- **説明:** `smb3`が存在していてtrueの場合、デバイスのユーザはシステムのモバイルデバイス管理(MDM)制御に登録されています。このフィールドが存在すると、LocalPolicyで制御するSecure Enclaveプロセッサアプリケーションは、ローカルユーザ認証を要求する代わりにMDM認証を受け入れます。ユーザはこのフィールドを、起動セキュリティユーティリティまたは`bputil`を使用して、他社製のkextおよびソフトウェアアップデートの管理対象制御を有効にすることで変更できます。(macOS 11.2以降では、現在のセキュリティモードが「完全なセキュリティ」の場合、MDMで最新バージョンのmacOSへのアップデートを開始することもできます。)

安全なマルチブート(smb4)

- **型:** ブール値
- **変更可能な環境:** macOS
- **説明:** `smb4`が存在していてtrueの場合、デバイスは、Apple School Manager、Apple Business Manager、またはApple Business Essentialsを使用してオペレーティングシステムのMDM制御に登録されています。このフィールドが存在すると、Secure Enclaveアプリケーションを制御するLocalPolicyは、ローカルユーザ認証を要求する代わりにMDM認証を受け入れます。このフィールドは、デバイスのシリアル番号がそれら3つのサービスのいずれかに表示されていることを検出すると、MDMソリューションによって変更されます。

システム整合性保護(sip0)

- **型:** 64ビットの符号なし整数
- **変更可能な環境:** 1TR
- **説明:** `sip0`は、以前にNVRAMに保存された既存のシステム整合性保護(SIP)ポリシービットを保持します。新しいSIPポリシービットは、LLBではなくmacOSでのみ使用される場合、以下のようなLocalPolicyのフィールドを使用する代わりに、ここに追加されます。ユーザはこのフィールドを、1TRの`csrutil`を使用してSIPを無効にし、「セキュリティ制限なし」にダウングレードすることで変更できます。

システム整合性保護(sip1)

- **型:** ブール値
- **変更可能な環境:** 1TR
- **説明:** `sip1`が存在していてtrueの場合、iBootは、SSVボリュームのルートハッシュの検証に失敗することを許可します。ユーザはこのフィールドを、1TRから`csrutil`または`bputil`を使用することで変更できます。

システム整合性保護(sip2)

- **型:** ブール値
- **変更可能な環境:** 1TR
- **説明:** sip2が存在していてtrueの場合、iBootは、カーネルメモリに書き込み不可のマークを付ける**構成可能なテキスト読み取り専用領域(CTRR)**ハードウェアレジスタをロックしません。ユーザはこのフィールドを、1TRから`csrutil`または`bputil`を使用することで変更できます。

システム整合性保護(sip3)

- **型:** ブール値
- **変更可能な環境:** 1TR
- **説明:** `sip3`が存在していてtrueの場合、iBootはboot-args NVRAM変数の組み込み許可リストを適用しません。そうしない場合は、カーネルに渡されるオプションをフィルタします。ユーザはこのフィールドを、1TRから`csrutil`または`bputil`を使用することで変更できます。

証明書とRemotePolicy

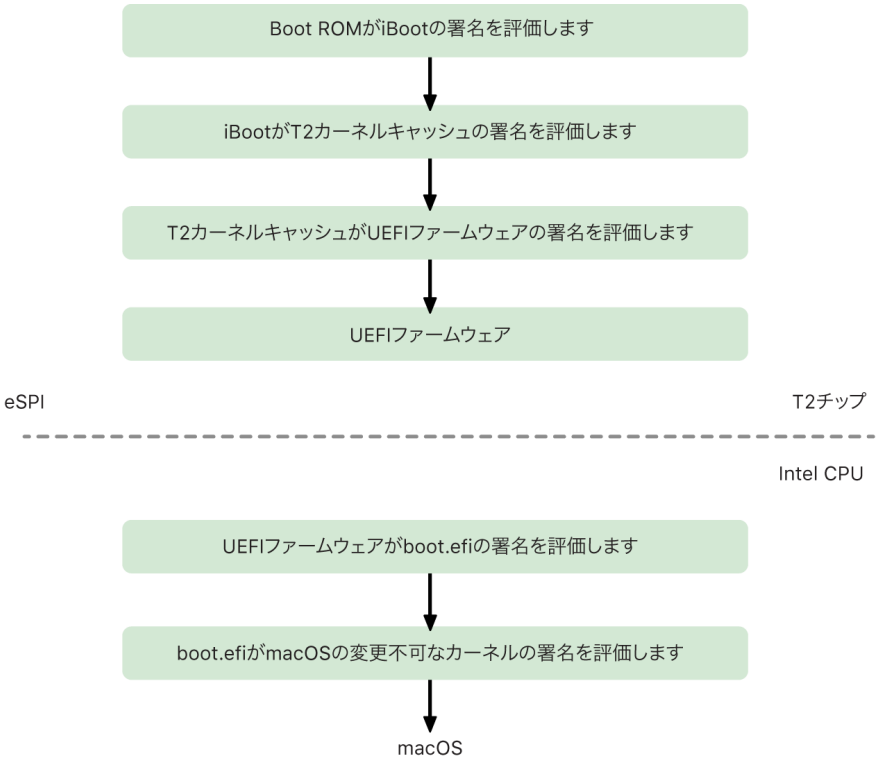
LocalPolicyの署名キーの作成と管理で説明されているように、LocalPolicyのImage4には、所有者ID証明書(OIC)と組み込みのRemotePolicyも含まれています。

Intelプロセッサ搭載Macコンピュータ

Intelプロセッサ搭載Macのブートプロセス

Apple T2セキュリティチップを搭載したIntelプロセッサ搭載Mac

Apple T2セキュリティチップおよびIntelプロセッサ搭載Macコンピュータの電源を入れると、チップはiPhone、iPad、およびAppleシリコン搭載Macと同じ方法で、Boot ROMからセキュアブートを実行します。これはiBootのブートローダーを確認し、信頼チェーンの最初のステップです。iBootはT2チップ上でカーネルとカーネル拡張機能のコードを確認してから、Intel UEFIファームウェアを確認します。UEFIファームウェアおよび関連する署名は、まずはT2チップでのみ使用できます。



検証の後、UEFIファームウェアのイメージがT2チップのメモリの一部にマップされます。このメモリは、拡張シリアルペリフェラルインターフェイス（eSPI）を通じてIntel CPUで使用できるようになります。Intel CPUは自身の最初の起動時に、T2チップ上の、整合性が確認され、メモリにマップされたファームウェアのコピーから、eSPIを通じてUEFIファームウェアを取得します。

信頼チェーンの評価はIntel CPUで継続されます。UEFIファームウェアがboot.efi（macOSのブートローダー）の署名を評価します。Intelのアプリプロセッサに常駐するmacOSのセキュアブート用の署名はiOS、iPadOS、T2チップのセキュアブートに使用されているものと同じImage4形式で保存されます。Image4ファイルを解析するコードは、現在のiOSおよびiPadOSのセキュアブート実装のものと同じ、ハードコーディングされたコードです。次に、boot.efiはimmutablekernelという新しいファイルの署名を検証します。セキュアブートが有効になっているとき、immutablekernelファイルはmacOSの起動に必要なAppleのカーネル拡張機能の完全なセットとなります。セキュアブートポリシーはimmutablekernelにプロセスが引き継がれた時点で終了します。その後はmacOSのセキュリティポリシー（システム整合性保護や署名されたカーネル拡張機能など）が有効になります。

このプロセスでエラーまたは失敗が起きると、Macが復元モード、Apple T2セキュリティチップのリカバリモード、またはApple T2セキュリティチップのデバイスファームウェアアップグレード（DFU）モードに入ります。

T2チップおよびIntelプロセッサ搭載Mac上のMicrosoft Windows

デフォルトでは、セキュアブートをサポートするIntelプロセッサ搭載Macは、Appleによって署名されたコンテンツのみを信頼します。ただし、Boot Campでインストールしたオペレーティングシステムのセキュリティを向上させるため、AppleはWindowsのセキュアブートもサポートしています。Unified Extensible Firmware Interface（UEFI）ファームウェアにはMicrosoftのブートローダーの認証に使用するMicrosoft Windows Production CA 2011証明書のコピーが含まれています。

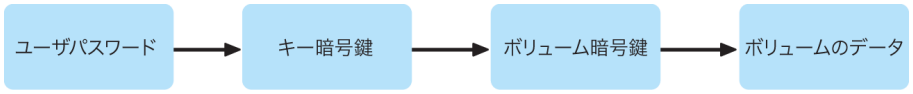
注記: Microsoft Corporation UEFI CA 2011は、Microsoft社のパートナーによって署名されたコードの検証を許可する証明書ですが、現時点でこれに対する信頼性は確立されていません。一般にこのUEFI CAは、Linuxのバリアントなどのオペレーティングシステムでブートローダーの真正性を検証する際に使用されています。

デフォルトではWindowsのセキュアブートのサポートは有効になっていませんが、Boot Campアシスタント（BCA）を使用すれば有効になります。ユーザがBCAを実行すると、macOSはファーストパーティのMicrosoft社が署名したコードを起動時に信頼するよう再構成されます。BCAの完了後、macOSがセキュアブート時にAppleによるファーストパーティの信頼性評価に合格しなかった場合は、UEFIファームウェアはUEFIセキュアブートのフォーマットに応じてオブジェクトの信頼性の評価を試みます。信頼性の評価に成功すると、Macでプロセスが続行され、Windowsが起動します。成功しなかった場合は、MacがrecoveryOSに切り替わり、信頼性の評価に失敗したことをユーザに通知します。

T2チップを搭載していないIntelプロセッサ搭載Macコンピュータ

T2チップを搭載していないIntelプロセッサ搭載Macはセキュアブートをサポートしていません。このため、Unified Extensible Firmware Interface（UEFI）ファームウェアはファイルシステムからmacOSの起動システム（boot.efi）を検証なしに読み込み、起動システムはファイルシステムからカーネル（prelinkedkernel）を検証なしに読み込みます。ブートチェーンの整合性を保護するために、ユーザは以下のすべてのセキュリティ機能を有効にする必要があります:

- **システム整合性保護（SIP）:** デフォルトで有効になっています。これによって、実行中のmacOSでの悪質な書き込みから起動システムとカーネルが保護されます。
- **FileVault:** ユーザが有効にすることも、モバイルデバイス管理（MDM）の管理者が有効にすることもできます。これによって、Macに物理的にアクセスできる攻撃者がターゲットディスクモードを使用して起動システムを上書きすることを防止できます。
- **ファームウェアパスワード:** ユーザが有効にすることも、MDMの管理者が有効にすることもできます。これによって、物理的に存在する攻撃者が、recoveryOSやシングルユーザモード、ターゲットディスクモードなどの別のブートモードを起動して、起動システムを上書きすることを防止できます。また、攻撃者は別のメディアを使用してコードを実行し、起動システムを上書きすることがありますが、こうした別のメディアからの起動も防止できます。



Apple T2セキュリティチップを搭載したIntelプロセッサ搭載Macコンピュータのブートモード

Apple T2セキュリティチップおよびIntelプロセッサ搭載Macには、さまざまなブートモードがあります。ブート時にキーを組み合わせて押すとUEFIファームウェアまたはブートシステムによってモードが認識され、そのモードに入ります。シングルユーザモードなどの一部のブートモードは、起動セキュリティユーティリティでセキュリティポリシーを「セキュリティなし」に変更しないと動作しません。

モード	キーの組み合わせ	説明
macOSの起動	なし	UEFIファームウェアからmacOSのブートシステム（UEFIアプリケーション）にプロセスが引き継がれます。ブートシステムからはmacOSカーネルにプロセスが引き継がれます。FileVaultが有効になっているMacの標準的なブートでは、macOSのブートシステムは、ストレージを復号するパスワードを取得するログインウインドウインターフェイスを表示します。
Startup Manager	Optionキー（⌥）	UEFIファームウェアによって内蔵のUEFIアプリケーションが起動します。UEFIアプリケーションはブートデバイスを選択するためのインターフェイスをユーザに提示します。
ターゲットディスクモード（TDM）	Tキー	UEFIファームウェアによって内蔵のUEFIアプリケーションが起動します。UEFIアプリケーションは、FireWire、Thunderbolt、USB、またはこの3つの組み合わせ（Macのモデルによって異なります）を通じて、内部ストレージデバイスをブロックベースの生のストレージデバイスとして提示します。
シングルユーザモード	Command（⌘）+Sキー	macOSカーネルがlaunchdの引数ベクトル内に–sフラグを渡したあと、launchdがコンソールアプリのttyにシングルユーザシェルを作成します。 **注記:** ユーザがシェルを終了すると、macOSはログインウインドウのブートを続けます。
recoveryOS	Command（⌘）+Rキー	UEFIファームウェアは内部ストレージデバイスにある署名付きのディスクイメージ（.dmg）ファイルから最小限のmacOSを読み込みます。
インターネットrecoveryOS	Option（⌥）+Command（⌘）+Rキー	HTTPを使用してインターネットから署名付きのディスクイメージがダウンロードされます。
診断	Dキー	UEFIファームウェアは内部ストレージデバイスにある署名付きのディスクイメージファイルから最小限のUEFI診断環境を読み込みます。
インターネット診断	オプション（⌥）+Dキー	HTTPを使用してインターネットから署名付きのディスクイメージがダウンロードされます。
Windowsの起動	なし	Boot Campを使用してWindowsがインストールされている場合、UEFIファームウェアからWindowsのブートシステムにプロセスが引き継がれたあと、WindowsのブートシステムからWindowsカーネルにプロセスが引き継がれます。

Apple T2セキュリティチップを搭載したMacの起動セキュリティユーティリティ

概要

Apple T2セキュリティチップおよびIntelプロセッサ搭載Macでは、起動セキュリティユーティリティは多くのセキュリティポリシー設定を管理します。このユーティリティには、recoveryOSをブートし、「ユーティリティ」メニューから「起動セキュリティユーティリティ」を選択することでアクセスでき、サポートされているセキュリティ設定を攻撃者による安易な操作から保護します。

重要なポリシーの変更には認証が必要です。リカバリモードのときでも同様です。起動セキュリティユーティリティを初めて開いたとき、ユーザはブート中のrecoveryOSに関連付けられているプライマリmacOSの管理者パスワードの入力を求められます。管理者がいない場合、ポリシーを変更するには管理者を作成しておく必要があります。T2チップは、現在Macコンピュータがリカバリ中であり、こうしたポリシー変更の前にSecure Enclaveに基づいた資格情報による認証が行われていることを要求します。セキュリティポリシーの変更には2つの暗黙要件があります。recoveryOSは以下の条件を満たす必要があります:

- T2チップに直接接続されているストレージデバイスから起動している。これは、ほかのデバイス上のパーティションには、内蔵ストレージデバイスにバインドされたSecure Enclaveに基づく資格情報がないためです。
- APFSベースのボリューム上にある。これは、Secure Enclaveに送信される復元時認証の資格情報の保存が、ドライブの「プリブート」APFSボリューム上でのみサポートされるためです。HFS+フォーマットのボリュームではセキュアブートを使用できません。

このポリシーは、T2チップを搭載したIntelプロセッサ搭載Macの起動セキュリティユーティリティにのみ表示されます。ほとんどのユースケースではセキュアブートポリシーの変更が不要ですが、デバイスの設定を最終的に制御するのはユーザであり、ユーザは必要に応じてMacのセキュアブート機能を無効にするかダウングレードすることを選択できます。

このアプリ内から行われたセキュアブートポリシーの変更は、Intelプロセッサで検証される信頼チェーンの評価にのみ適用されます。「T2チップのセキュアブート」オプションは常に有効です。

セキュアブートポリシーは、「完全なセキュリティ」、「中程度のセキュリティ」、「セキュリティなし」の3つのいずれかに設定できます。「セキュリティなし」に設定すると、Intelプロセッサでのセキュアブートの評価が完全に無効になり、ユーザが任意のOSを起動できます。

「完全なセキュリティ」のブートポリシー

「完全なセキュリティ」はデフォルトのブートポリシーであり、iOSとiPadOS、またはAppleシリコン搭載Macの「完全なセキュリティ」と同様に動作します。ソフトウェアがダウンロードされてインストールできるようになった時点で、署名リクエストの一部としてECID（Exclusive Chip Identification）が含まれる署名を使ってパーソナライズされます。この場合のECIDとは、T2チップごとに固有のIDです。署名サーバから送り返される署名は一意になり、署名を要求したT2チップのみで使用できます。Unified Extensible Firmware Interface（UEFI）ファームウェアは、「完全なセキュリティ」のポリシーが有効な場合に、提供された署名がAppleによるものということだけでなく、そのMacのみのために署名されていて、実質的にそのバージョンのmacOSをそのMacに関連付けるものであることを保証するように設計されています。これは、Appleシリコン搭載Macでの「完全なセキュリティ」についての説明のように、ロールバック攻撃を防ぐのに役立ちます。

「中程度のセキュリティ」のブートポリシー

「中程度のセキュリティ」のブートポリシーでは、従来のUEFIセキュアブートと同様の状況になります。ベンダー（この場合はApple）から提供されたコードであることを保証するために、ベンダーがコードのデジタル署名を生成します。この方法で、攻撃者が無署名のコードを挿入することを阻止できます。Appleではこの署名を「グローバル」署名と呼びます。この署名は現在「中程度のセキュリティ」のポリシーが設定されている任意のMacで任意の期間使用できるからです。iOS、iPadOS、およびT2チップ自体はいずれもグローバル署名をサポートしていません。この設定はロールバック攻撃の防止を試みません。

メディアのブートポリシー

メディアのブートポリシーは、T2チップおよびIntelプロセッサ搭載Macにのみ存在し、セキュアブートポリシーからは独立しています。そのため、ユーザがセキュアブートを無効にしても、T2チップに直接接続されているストレージデバイス以外からMacをブートしないようにするというデフォルトの動作は変更されません。（メディアのブートポリシーはAppleシリコン搭載Macでは必要ありません。詳しくは、起動ディスクのセキュリティポリシー管理を参照してください。）

Intelプロセッサ搭載Macのファームウェアパスワードの保護

Apple T2セキュリティチップを搭載したIntelプロセッサ搭載Macコンピュータ上のmacOSは、特定のMacでのファームウェア設定が意図せず変更されることを防止するためにファームウェアパスワードを使用することをサポートしています。ファームウェアパスワードは、recoveryOSまたはシングルユーザモードでのブート、不正なボリュームからのブート、ターゲットディスクモードでのブートなどの代替起動モードが選択されることを防止するためのものです。

注記: Appleシリコン搭載Macでは、ファームウェアパスワードは必要ありません。これは、制限されていた重要なファームウェア機能がrecoveryOSに移動され、（FileVaultが有効になっている場合）重要な機能にアクセスする前にrecoveryOSがユーザの承認を要求するためです。

ファームウェアパスワードの最も基本的なモードは、T2チップを**搭載していない**MacではrecoveryOSのファームウェアパスワードユーティリティから、T2チップ**および**Intelプロセッサ搭載Macでは起動セキュリティユーティリティから利用できます。詳細オプション（起動のたびにパスコードを要求する機能など）は、macOSの`firmwarepasswd`コマンドラインツールから利用できます。

ファームウェアパスワードの設定は、T2チップを搭載していないIntelプロセッサ搭載Macコンピュータで物理的に存在する攻撃者から攻撃を受けるリスクを低減するために特に重要です。ファームウェアパスワードを設定すると、攻撃者がシステム整合性保護（SIP）を無効にする可能性のあるrecoveryOSをブートすることを阻止できます。また、代替メディアの起動の制限により、攻撃者は別のオペレーティングシステムから特権コードを実行してペリフェラルファームウェアを攻撃することができません。

ファームウェアパスワードには、パスワードを忘れてしまったユーザのためのリセットメカニズムが用意されています。ユーザが起動時に特定の組み合わせのキーを押すと、AppleCareに提供するためのモデル固有の文字列が表示されます。AppleCareは、Uniform Resource Identifier（URI）によって署名が確認されたリソースにデジタル署名します。この署名が検証され、内容がそのMac用のものであれば、UEFIファームウェアによってファームウェアパスワードが削除されます。

自分以外のだれもソフトウェアでファームウェアパスワードを削除できないようにしたいユーザのために、macOS 10.15の`firmwarepasswd`コマンドラインツールに`-disable-reset-capability`オプションが追加されました。ユーザはこのオプションを設定する前に、パスワードを忘れてパスワードの削除が必要になった場合にかかるロジックボード交換の費用を自ら負担することを承認する必要があります。組織のMacコンピュータを外部の攻撃者からも従業員からも保護したい場合は、組織が所有するシステムにファームウェアパスワードを設定する必要があります。これは以下のいずれかの方法でデバイス上で実行できます:

- プロビジョニング時に手動で`firmwarepasswd`コマンドラインツールを使用する
- `firmwarepasswd`コマンドラインツールを使用する他社製管理ツールを利用する
- モバイルデバイス管理(MDM)を使用する

Intelプロセッサ搭載MacのrecoveryOSおよび診断環境

recoveryOS

recoveryOSはメインのmacOSとは完全に分離されていて、recoveryOSの内容はすべてBaseSystem.dmgという名前のディスクイメージファイルに保存されています。また、関連するファイルとして、BaseSystem.dmgの整合性の検証に使用するBaseSystem.chunklistもあります。chunklistは、BaseSystem.dmgの10 MBチャンクのハッシュリストです。Unified Extensible Firmware Interface(UEFi)ファームウェアはchunklistファイルの署名を評価したあと、BaseSystem.dmgのハッシュを一度に1チャンクずつ評価します。これにより、chunklistに記されている署名付きコンテンツと一致することを確認できます。一致しないハッシュがあると、ローカルのrecoveryOSからのブートは中断され、UEFIファームウェアはインターネットrecoveryOSからのブートを試みます。

検証が問題なく完了すると、UEFIファームウェアはBaseSystem.dmgをRAMディスクとしてマウントし、ここに含まれるboot.efiを起動します。UEFIファームウェアがboot.efiを詳細に確認する必要はなく、boot.efiがカーネルを確認する必要もありません。オペレーティングシステムの全コンテンツの整合性はすでに確認されているためです(これらの要素はOSの構成要素です)。

Apple Diagnostics

ローカルの診断環境を起動する手順はrecoveryOSの起動の手順とほぼ同じです。AppleDiagnostics.dmgとAppleDiagnostics.chunklistという別個のファイルを使用しますが、検証方法はBaseSystemファイルのときと同じです。UEFIファームウェアは、boot.efiを起動するのではなく、ディスクイメージ(.dmgファイル)内にあるdiags.efiという名前のファイルを起動します。このファイルは、ほかの各種UEFIドライバを呼び出してハードウェアに接続し、ハードウェア内のエラーを確認する役割を担います。

インターネットrecoveryOSと診断環境

ローカルのリカバリまたは診断環境の起動中にエラーが発生すると、UEFIファームウェアはインターネットからイメージをダウンロードすることを試みます。(ユーザはブート時に特別なキーシーケンスを押したままにすることで、インターネットからイメージを取得することを明確に要求することもできます。)OS復旧サーバからダウンロードしたディスクイメージとchunklistの整合性の検証は、ストレージデバイスから取得したイメージの場合と同じ方法で行われます。

OS復旧サーバとの接続にはHTTPが使用されますが、ダウンロードしたすべてのコンテンツは前述の通りに整合性が確認されます。このため、ネットワークを制御して改ざんを試みる攻撃から保護されます。チャンクの1つが整合性の検証に失敗すると、OS復旧サーバからの要求を11回繰り返し、それでも失敗した場合は起動を断念してエラーを表示します。

2011年にインターネットリカバリモードと診断モードがMacコンピュータに追加されたとき、より単純なトランスポートを使用し、チャンクリストメカニズムを使用してコンテンツ認証を処理する方が、UEFIファームウェアでより複雑なHTTPS機能を実装し、その結果ファームウェアの攻撃対象領域が増えるよりもよいと判断されました。

署名済みシステムボリュームのセキュリティ

macOS 10.15では、Appleは、システムコンテンツ専用の分離されたボリュームである、読み取り専用システムボリュームを導入しました。macOS 11以降は、**署名済みシステムボリューム(SSV)**を含むシステムコンテンツに強力な暗号保護を追加します。SSVは、実行時にシステムコンテンツの整合性を検証し、Appleからの有効な暗号署名のないデータ(コードとコード以外)を拒否するカーネルメカニズムを備えています。iOS 15およびiPadOS 15以降では、iPhoneまたはiPadのシステムボリュームに署名済みシステムボリュームの暗号保護も追加されています。

SSVは、オペレーティングシステムの一部であるAppleソフトウェアの改ざんを防ぐだけでなく、macOSソフトウェアのアップデートの信頼性と安全性を高めます。また、SSVはAPFS(Apple File System)スナップショットを使用するため、アップデートを実行できない場合は、再インストールせずに古いシステムバージョンを復元できます。

導入以来、APFSは、内部ストレージデバイスで非暗号化チェックサムを使用してファイルシステムメタデータの整合性を確保してきました。SSVは、暗号学的ハッシュを追加し、ファイルデータのすべてのバイトを包含するように拡張することによって、整合性メカニズムを強化します。内部ストレージデバイスからのデータ(ファイルシステムのメタデータを含む)は、読み取りパスで暗号学的にハッシュ化されます。そのあと、ハッシュがファイルシステムメタデータの期待値と比較されます。一致しない場合、システムはデータが改ざんされていると見なし、要求元のソフトウェアに返しません。

各SSV SHA256ハッシュは、それ自体がハッシュ化されるメインのファイルシステムメタデータツリーに格納されます。また、ツリーの各ノードはその子のハッシュの整合性を再帰的に検証するため(バイナリハッシュ(Merkle)ツリーと同様)、ルートノードのハッシュ値(**シール**と呼ばれます)には、SSV内のデータのすべてのバイトが包含されます。つまり、暗号署名がシステムボリューム全体を保護します。

このシールは、macOSのインストールおよびアップデート中にデバイス上のファイルシステムから再計算され、その測定値はAppleが署名した測定値と照合されます。Appleシリコン搭載Macでは、ブートローダーは制御をカーネルに移す前にシールを検証します。Apple T2セキュリティチップおよびIntelプロセッサ搭載Macでは、ブートローダーが測定値と署名をカーネルに転送し、そのあとカーネルがルートファイルシステムをマウントする直前にシールを検証します。いずれの場合も、検証が失敗すると起動プロセスが停止し、ユーザはmacOSを再インストールするように求められます。この手順は、ユーザが低セキュリティモードに入ることを選択し、かつ、署名済みシステムボリュームを無効にすることを個別に選択した場合を除き、ブートするたびに繰り返されます。

iOSおよびiPadOSのソフトウェアアップデート中に、そのシステムボリュームは同様の方法で準備されて再計算されます。iOSとiPadOSのブートローダーは、シールが同じままであり、Appleが署名した値と一致することを検証してから、デバイスがカーネルを起動することを許可します。ブート時に不一致が確認されると、ユーザはデバイスのシステムソフトウェアをアップデートすることを求められます。ユーザが、iOSおよびiPadOSの署名済みシステムボリュームの保護を無効にすることは許可されません。

SSVとコード署名

コード署名は引き続き存在し、カーネルによって適用されます。署名済みシステムボリュームは、内蔵ストレージデバイスからいずれかのバイトが読み取られるときの保護機能を備えています。これに対し、コード署名では、Machオブジェクトが実行可能としてメモリにマップされたときの保護機能を備えています。SSVとコード署名は、両方とも、すべての読み取りパスと実行パスの実行可能コードを保護します。

SSVとFileVault

macOS 11以降では、保管中のシステムコンテンツに対し、同等の保護がSSVによって提供されるため、システムボリュームを暗号化する必要がなくなりました。保管中にファイルシステムに加えられた変更は、読み取られたときにファイルシステムによって検出されます。ユーザがFileVaultをオンにしている場合でも、データボリューム上のユーザのコンテンツは、ユーザが指定したシークレットで暗号化されます。

ユーザがSSVを無効にすることを選択した場合、保存時のシステムは改ざんに対して脆弱になります。この改ざんにより、攻撃者はシステムの次回の起動時に暗号化されたユーザデータを抽出できる可能性があります。したがって、FileVaultがオンになっている場合、システムはユーザがSSVを無効にすることを許可しません。保管中の保護は、一貫した方法で両方のボリュームに対して有効または無効にする必要があります。

macOS 10.15以前では、FileVaultは、ユーザが提供するシークレットで保護された鍵を使用してユーザおよびシステムコンテンツを暗号化することにより、保管中にオペレーティングシステムソフトウェアを保護します。これにより、デバイスに物理的にアクセスできる攻撃者が、システムソフトウェアが含まれているファイルシステムにアクセスしたり実質的に変更したりするのを防ぎます。

SSVとApple T2セキュリティチップを搭載したMac

Apple T2セキュリティチップを搭載したMacでは、macOS自体のみがSSVによって保護されます。T2チップで実行され、macOSを検証するソフトウェアは、セキュアブートによって保護されます。

安全なソフトウェアアップデート

セキュリティはプロセスです。工場出荷時にインストールされているオペレーティングシステムのバージョンを確実にブートするだけでは不十分です。最新のセキュリティアップデートを迅速かつ安全に取得するためのメカニズムも存在する必要があります。Appleは、新たなセキュリティ上の懸念に対処するために、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。iPhoneおよびiPadデバイスのユーザは、アップデートの通知をデバイスで受け取ります。Macユーザは、「システム設定」(macOS 13以降)または「システム環境設定」(macOS 12以前)で、利用できるアップデートを確認できます。最新のセキュリティ修正を迅速に導入できるように、アップデートはワイヤレスで配信されます。

アップデートプロセスのセキュリティ

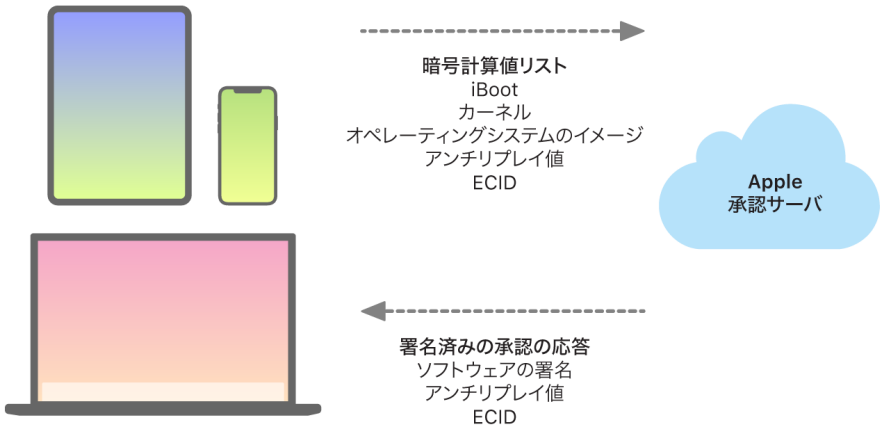
アップデートプロセスでは、セキュアブートで使用されるのと同じハードウェアベースの信頼ルートを使用し、Appleが署名したコードのみをインストールするように設計されています。また、アップデートプロセスでは、システムソフトウェア認証を使用して、Appleが能動的に署名したバージョンのオペレーティングシステムのコピーのみが、iPhoneおよびiPadデバイス、または起動セキュリティユーティリティでセキュアブートポリシーとして「完全なセキュリティ」が設定されているMacコンピュータにインストール可能であることも確認されます。これらの安全なプロセスを適切に使用することで、Appleは既知の脆弱性を持つ古いバージョンのオペレーティングシステムへの署名を停止でき、ダウングレード攻撃を防ぐことができます。

ソフトウェアアップデートのセキュリティを強化するため、アップグレードするデバイスが物理的にMacに接続されているときは、iOSまたはiPadOS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。ただし、ワイヤレス(OTA)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、オペレーティングシステム全体のダウンロードの回避によりネットワーク効率が向上します。さらに、macOS 10.13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、iPhoneおよびiPad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。)

パーソナライズされたアップデートプロセス

アップグレードおよびアップデート中に、Appleインストール認証サーバで利用可能になる情報があります。インストールしようとしているインストールバンドルの各部分（例えば、iBoot、カーネル、オペレーティングシステムイメージ）の暗号測定値のリスト、ランダムなアンチリプレイ値、デバイス固有のExclusive Chip Identification（ECID）などです。

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、一致が確認された場合は、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、ストレージデバイス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が検証されます。これは、パーソナライズをサポートするデバイスで認証が特定のデバイスに対するものであることと、あるデバイスの古いバージョンのオペレーティングシステムまたはファームウェアを別のデバイスにコピーできないことを保証するための手順です。また、アンチリプレイ値が使用されるため、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。

Appleが設計したシリコン（セキュリティチップおよびIntelプロセッサ搭載Macなど）で、デバイスをアップデートするために常にAppleへのネットワーク接続が必要となるのは、パーソナライズプロセスを実行するためです。

Secure Enclaveを備えたデバイスでは、そのハードウェアで同様にシステムソフトウェア認証が使用されます。これはソフトウェアの整合性を確認する機能であり、ダウングレード目的のインストールを防止するように設計されています。

オペレーティングシステムの整合性

Appleのオペレーティングシステムソフトウェアはセキュリティを中核として設計されています。この設計には、セキュアブートを可能にするために活用できるハードウェア信頼ルートと、迅速かつ安全なソフトウェアアップデートプロセスが含まれます。Appleのオペレーティングシステムでは、オペレーティングシステムの実行時の悪用を防ぐため、専用のシリコンベースのハードウェア機能も使用されます。これらの実行時の機能により、オペレーティングシステムの実行時に信頼できるコードの整合性が保護されます。つまり、Appleのオペレーティングシステムソフトウェアでは、悪質なアプリ、Web、またはその他のチャネルから実行される攻撃や悪用テクニックによる影響を軽減できます。ここに記載されている保護機能は、Appleが設計したSoCがサポートされているデバイスで利用できます。これにはiOS、iPadOS、tvOS、watchOSが含まれ、Appleシリコン搭載Mac上のmacOSも含まれるようになりました。

機能	A10	A11、S3	A12、A13、A14 S4–S9	A15、A16、A17	M1、M2、M3
カーネル整合性保護	✓	✓	✓	✓	✓
高速許可制限	✗	✓	✓	✓	✓
システムコプロセッサ整合性保護	✗	✗	✓	✓	✓
ポインタ認証コード	✗	✗	✓	✓	✓
ページ保護レイヤー	✗	✓	✓	✓	✗ 以下の注記1を参照。
Secure Page Table Monitor	✗	✗	✗	✓ 以下の注記2を参照。	✗

注記1: ページ保護レイヤー(PPL)では、プラットフォームが署名済みの信頼できるコード**のみを**実行する必要があります。このセキュリティモデルは、macOSには該当しません。

注記2: SPTM(Secure Page Table Monitor)はA15、A16、およびA17で対応していて、対応するプラットフォームでページ保護レイヤーに代わるものです。

カーネル整合性保護

オペレーティングシステム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拡張機能を読み込みます。起動が完了したあとは、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。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。

構成変更を防ぐため、KIPの有効化に使用されるハードウェアはブートプロセス完了後にロックされます。

高速許可制限

Apple A11 BionicおよびS3 SoCから、新しいハードウェアプリミティブが導入されました。このプリミティブ、高速許可制限には、スレッドごとに権限を素早く制限するCPUレジスタが採用されています。高速許可制限(APRRレジスタとも呼ばれます)により、サポートされているオペレーティングシステムは、システムコールおよびページテーブルのウォーク/フラッシュのオーバーヘッドを発生させずに実行権限をメモリから削除できます。これらのレジスタは、Webからの攻撃、特に実行時にコンパイル(ジャストインタイムコンパイル)されたコードによる攻撃による影響を軽減するもう1つの手段となります。これは、メモリが読み取りおよび書き込みされているときにメモリを効果的に実行できないためです。

システムコプロセッサ整合性保護

コプロセッサのファームウェアによって、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などの多数の重要なシステムタスクが処理されます。したがって、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。コプロセッサファームウェアの変更を防ぐために、Appleは**システムコプロセッサ整合性保護(SCIP)**と呼ばれるメカニズムを使用しています。

SCIPはカーネル整合性保護(KIP)と同様に機能します。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

また、ブート時に、Secure EnclaveのSCIPを構成するためにSecure Enclaveオペレーティングシステムが使用されます。SCIPの有効化に使用されるハードウェアはブートプロセス完了後にロックされます。これは構成変更を防ぐためです。

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を防ぐために使用されます。システムソフトウェアおよび内蔵アプリは、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。PACでは、5つの128ビットシークレット値を使用してカーネル命令とデータに署名し、ユーザ領域プロセスごとに固有のBキーが生成されます。項目は以下のようにソルト化され、署名されます。

項目	キー	ソルト
関数のリターンアドレス	IB	ストレージアドレス
関数ポインタ	IA	0
ブロック呼び出し関数	IA	ストレージアドレス
Objective-Cメソッドキャッシュ	IB	ストレージアドレス + クラス + セレクタ
C++ Vテーブルエントリ	IA	ストレージアドレス + ハッシュ(マングルされたメソッド名)
計算済みGotoラベル	IA	ハッシュ(関数名)
カーネルスレッドの状態	GA	・
ユーザスレッドの状態レジスタ	IA	ストレージアドレス
C++ Vテーブルポインタ	DA	0

署名値は、64ビットポインタの最上位にある未使用のパディングビットに格納されます。署名は使用される前に検証され、ポインタアドレスが機能するようにパディングが復元されます。検証に失敗すると、中止されます。この検証によって、ROP(Return-Oriented Programming)攻撃などの多くの攻撃の難易度が高まります。ROP攻撃は、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ものです。

ページ保護レイヤー

iOS、iPadOS、およびwatchOSのページ保護レイヤー(PPL)は、コード署名の検証が完了したあと、ユーザ領域のコードが改ざんされるのを防ぐように設計されています。PPLは、カーネル整合性保護および高速許可制限を基盤として、ページテーブルへのアクセス権の無効化を管理し、ユーザコードとページテーブルを含む保護されたページをPPLのみが変更できるようにします。このシステムでは、カーネルが侵害された場合でもシステム全体でのコードの整合性が確保されるため、攻撃対象領域が大幅に狭まります。PPLは実行されるすべてのコードが署名されている必要があるシステムにのみ適用されるため、この保護はmacOSでは提供されていません。

Secure Page Table MonitorとTrusted Execution Monitor

Secure Page Table Monitor(SPTM)とTrusted Execution Monitor(TXM)は、攻撃者がカーネル書き込み機能を持っていて、制御フロー保護をバイパスできる場合でも、ユーザとカーネルプロセスの両方のページテーブルを改ざんから保護するために連携するよう設計されています。SPTMは、カーネルより高い権限レベルを利用し、権限がより低いTXMを利用してコード実行を統治するポリシーを実際に適用することで、これを実行します。このシステムは、この権限分離と両者の間の信頼の統治によって、TXMの侵害がSPTMバイパスに自動的に変換されないように設計されています。 A15、A16、およびA17 SOCでは、SPTM(とTXM)がPPLに置き換わり、攻撃対象領域を小さくして防御しやすく、初期ブート時でもカーネルの信頼性に依存しないようになっています。また、SPTMは、PPLが利用する高速許可制限を進化させた、新しいシリコンプリミティブに依存します。

データ接続の安全な有効化

iPhone、iPad、Macコンピュータで、最近確立されたデータ接続がない場合、ユーザはFace ID、Touch ID、パスコードのいずれかを使用して、Thunderbolt、USB、Lightning、Smart Connector、または「SDXC」(SD eXtended Capacity)カード(macOS 13.3以降の場合)のインターフェイス経由のデータ接続を有効化する必要があります。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ほかのアクセサリの使いやすさも保てるようになります。iPhoneまたはiPadのロック後またはアクセサリのデータ接続の終了後1時間以上経つと、デバイスのロックを解除するまで、新たなデータ接続は一切確立できなくなります。この1時間の制限中は、デバイスがロック解除されていたときにすでに接続していたアクセサリからのデータ接続のみが許可されます。これらのアクセサリは、最後の接続後、30日間記憶されます。この制限中に不明なアクセサリからデータ接続の確立要求があると、デバイスのロックが再び解除されるまで、それらの接続を介したすべてのアクセサリのデータ接続が無効になります。この1時間という制限には次の利点があります。

- Mac、PC、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
- 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ための、暗号化を使った信頼できる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、アクセサリとのデータ接続が確立されてから3日以上経過している場合は、デバイスのロック後ただちに、新たなデータ接続を確立できなくなります。これにより、データ接続をするアクセサリ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、これらのデータ接続が無効になります。

ユーザは、「設定」で常時のデータ接続を再度有効にできます。また、一部の補助装置では、設定時に自動的に有効になります。

iPhoneおよびiPad用のアクセサリの検証

Made for iPhone/iPad（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)および必須の対応ハードウェアコンポーネントを利用できます。

MFiアクセサリがiPhoneまたはiPadと通信するとき、アクセサリは審査を通過したことをAppleに証明する必要があります。（アクセサリとデバイスの接続には、Thunderbolt、Lightning、Bluetooth、または特定のデバイスではUSB-Cを使用します。）アクセサリは、承認の証明としてApple発行の証明書をデバイスに送信し、そのあとデバイスが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。

検証済みMFiアクセサリは、別の伝送方法や伝送機能へのアクセス（Thunderbolt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は、認定MFiアクセサリにのみデバイスへのフルアクセスを付与しやすいように設計されています。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）を使用して、アクセサリとデバイス間の通信がAES128のカウンタ（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。

「メッセージ」とIDS用のBlastDoor

iOS、iPadOS、macOS、およびwatchOSには、iOS 14および関連リリースで初めて導入された、**BlastDoor**というセキュリティ機能が組み込まれています。BlastDoorの目標は、「メッセージ」とApple Identity Services（IDS）を悪用する操作を複雑にし、攻撃者を囲い込むことで、システムを保護することです。BlastDoorは、攻撃を防ぐために、「メッセージ」やIDSなどのベクトルに着信する信頼できないデータを分離、解析、トランスコード、および検証します。

BlastDoorは、サンドボックスの制限と出力のメモリ安全性検証を利用して大きな障害物を作ることによって、これを行います。攻撃者はそれを克服しないと、オペレーティングシステムのほかの部分に到達できません。攻撃に対するユーザ保護を大幅に改善するように設計されており、ユーザの操作を必要としない「ゼロクリック」攻撃に対して特に効果を発揮します。

さらに、「メッセージ」は「既知の送信者」からのトラフィックと「未知の送信者」からのトラフィックを分けて扱うので、それぞれのグループに異なる機能群を提供し、「既知」と「未知」のデータを専用のBlastDoorインスタンスに分割することができます。

Appleデバイスのロックダウンモードのセキュリティ

ロックダウンモードは、その立場や活動内容から、金銭目的の標的型スパイウェアなどの極めて精巧なデジタル脅威の標的になる可能性のあるごく一部の個人を対象に考案された、任意で使える究極のセキュリティ対策です。ほとんどの人はこの類の攻撃の標的になることはありません。

ロックダウンモードをオンにすると、デバイスは通常通りに機能しなくなります。潜在的に侵害される可能性のある攻撃対象領域を減らすため、セキュリティのために特定のアプリ、Webサイト、および機能が厳密に制限され、一部の操作はまったく利用できなくなることがあります。

ロックダウンモードはiOS 16以降、iPadOS 16以降、macOS 13以降、およびwatchOS 10以降で利用できます。iOS 17以降、iPadOS 17以降、macOS 14以降、およびwatchOS 10.1以降のアップデートでは、追加の保護機能を利用できます。ロックダウンモードの追加機能を活用するには、デバイスを最新のオペレーティングシステムにアップデートする必要があります。詳しくは、Appleサポートの記事「ロックダウンモードについて」を参照してください。

ロックダウンモードでは、セキュリティが向上するトレードオフとして、機能、パフォーマンス、あるいはその両方が犠牲になります。このトレードオフは、以下に影響します:

- バックグラウンドサービス
- 接続
- デバイス管理
- FaceTime
- Game Center
- メール
- メッセージ
- 写真
- Safari
- システム設定
- WebKit

macOSシステムのセキュリティのその他の機能

macOSシステムのセキュリティのその他の機能

macOSは、幅広いハードウェアセット（例えば、Intelプロセッサ搭載CPU、Apple T2セキュリティチップと組み合わせたIntelプロセッサ搭載CPU、およびAppleシリコン搭載SoC）で動作し、さまざまな汎用コンピューティングのユースケースをサポートしています。基本的なプリインストールされたアプリまたはApp Storeから入手できるアプリのみを使用するユーザもいますが、最高レベルの信頼で実行されるコードを実行およびテストできるように、本質的にすべてのプラットフォーム保護を無効にする必要があるカーネルハッカーであるユーザもいます。ほとんどはその中間であり、その多くが、さまざまなレベルのアクセスを必要とするペリフェラルとソフトウェアを持っています。AppleはmacOSプラットフォームを設計する上で、ハードウェア、ソフトウェア、サービスにわたって統合されたアプローチを採用しました。これは、設計自体でセキュリティを確保し、構成、導入、管理を簡素化しながら、ユーザが求める構成を可能にするプラットフォームです。macOSには、ITプロフェッショナルが企業データを保護し、安全な企業ネットワーク環境内に統合するために必要となる重要なセキュリティ技術も組み込まれています。

次の機能は、macOSユーザのさまざまなニーズをサポートし、それらを保護するのに役立ちます。以下のものが含まれます:

- 署名済みシステムボリュームのセキュリティ
- システム整合性保護
- 信頼キャッシュ
- ペリフェラルの保護
- AppleシリコンMacのRosetta 2（自動変換）のサポートとセキュリティ
- DMAのサポートと保護
- カーネル拡張機能（kext）のサポートとセキュリティ
- オプションROMのサポートとセキュリティ
- IntelプロセッサMacコンピュータのUEFIファームウェアのセキュリティ

システム整合性保護

macOSは、カーネルのアクセス許可を利用して、**システム整合性保護（SIP）**と呼ばれる機能で重要なシステムファイルの書き込み可能性を制限します。この機能は、Appleシリコン搭載Macで利用可能なハードウェアベースのカーネル整合性保護（KIP）とは別個の追加されたものであり、メモリ内のカーネルの変更を保護します。強制アクセス制御テクノロジーを活用して、システム整合性保護に加えて、サンドボックスやData Vaultなどのその他の多くのカーネルレベルの保護を提供します。

強制アクセス制御

macOSでは、強制アクセス制御が使用されます。これは、セキュリティの制限を定めた上書きできないポリシーであり、デベロッパによって作成されます。このアプローチは、ユーザが自らの必要に応じてセキュリティポリシーを無効化することが許可される、自由裁量のアクセス制御とは異なります。

強制アクセス制御はユーザには不可視ですが、サンドボックス化、ペアレンタルコントロール、管理対象の環境設定、機能拡張、システム整合性保護などの重要な機能を実現するのに役立つ、基盤となるテクノロジーです。

システム整合性保護

システム整合性保護では、ファイルシステム内の特定の重要な場所でコンポーネントを読み取り専用に制限して、悪質なコードによって改ざんされないようにします。システム整合性保護はコンピュータ固有の設定であり、ユーザがOS X 10.11以降にアップグレードするとデフォルトでオンになります。Intelプロセッサ搭載Macでは、これを無効にすると、物理ストレージデバイス上のすべてのパーティションが保護されなくなります。macOSでは、サンドボックス化されて実行されているか、管理者特権で実行されているかにかかわらず、システム上で実行されているすべてのプロセスに、このセキュリティポリシーが適用されます。

信頼キャッシュ

セキュアブートチェーンに含まれるオブジェクトの1つは、静的信頼キャッシュです。これは、署名済みシステムボリュームにマスターされているすべてのMach-Oバイナリの信頼できるレコードです。各Mach-Oは、コードディレクトリのハッシュで表されます。これらのハッシュは、効率的な検索のために、信頼キャッシュに挿入される前に並べ替えられます。コードディレクトリは、`codesign(1)`によって実行される署名操作の結果です。信頼キャッシュを適用するには、SIPを有効のままにする必要があります。Appleシリコン搭載Macで信頼キャッシュの適用を無効にするには、セキュアブートを「セキュリティ制限なし」に設定する必要があります。

バイナリが実行されると（新しいプロセスを生成する、または実行可能コードを既存のプロセスにマッピングする処理の一部として）、そのコードディレクトリが抽出されてハッシュされます。結果として生じるハッシュが信頼キャッシュで見つかった場合、バイナリ用に作成された実行可能マッピングにはプラットフォーム権限が付与されます。つまり、それらは任意の資格を持ち、署名の真正性についてそれ以上検証されずに実行される可能性があります。これは、バイナリに署名するApple証明書によってプラットフォーム特権がオペレーティングシステムのコンテンツに伝達されるIntelプロセッサ搭載Macとは対照的です。（この証明書は、バイナリが所有できる資格を制限しません。）

プラットフォーム以外のバイナリ（公証を受けた他社製のコードなど）を実行するには、有効な証明書チェーンが必要です。バイナリが所有する資格は、Apple Developer Programによってデベロッパに発行された署名プロファイルによる制約を受けます。

出荷時にmacOS内にあるすべてのバイナリは、**プラットフォーム識別子**で署名されています。Appleシリコン搭載Macでは、この識別子を使用して、バイナリがAppleによって署名されている場合でも、実行するにはそのコードディレクトリのハッシュが信頼キャッシュに存在する必要があることを示します。Intelプロセッサ搭載Macでは、古いリリースのmacOSから対象を絞ったバイナリの失効を実行するために、プラットフォーム識別子が使用されます。このような対象を絞った失効により、それらのバイナリが新しいバージョンで実行されることを防止できます。

静的信頼キャッシュは、バイナリのセットを特定のバージョンのmacOSに完全にロックします。この動作により、Appleが正規に署名した古いオペレーティングシステムのバイナリを、攻撃者がメリットを得るために新しいオペレーティングシステムに導入するのを防ぐことができます。

オペレーティングシステムの外部で提供されるプラットフォームコード

Appleは、プラットフォーム識別子で署名されていないバイナリ（Xcodeや開発ツールのスタックなど）を提供しています。それでも、AppleシリコンMacおよびT2チップを搭載したMacでは、プラットフォーム特権を使用して実行することが引き続き許可されています。このプラットフォームソフトウェアはmacOSとは独立して提供されるため、静的信頼キャッシュによって課される失効動作の影響を受けません。

読み込み可能な信頼キャッシュ

Appleでは、**読み込み可能な信頼キャッシュ**を備えたソフトウェアパッケージを提供しています。これらのキャッシュは、静的信頼キャッシュと同じデータ構造を持っています。ただし、静的信頼キャッシュは1つしかなく、カーネルの初期の初期化が完了したあとはその内容が常に読み取り専用範囲にロックされることが保証されていますが、実行時に読み取り可能な信頼キャッシュがシステムに追加されます。

これらの信頼キャッシュは、ブートファームウェアを認証するのと同じメカニズム(Appleの信頼できる署名サービスを使用したパーソナライズ)でまたはグローバルに署名されたオブジェクト(署名によって特定のデバイスにバインドされない)として認証されます。

パーソナライズされた信頼キャッシュの一例は、Appleシリコン搭載Macで現場での診断を実行するために使用されるディスクイメージと共に提供されるキャッシュです。この信頼キャッシュは、ディスクイメージと共にパーソナライズされ、診断モードでブートされている間に対象のMacコンピュータのカーネルに読み込まれます。この信頼キャッシュにより、ディスクイメージ内のソフトウェアをプラットフォーム特権で実行できます。

グローバルに署名された信頼キャッシュの一例は、macOSソフトウェアアップデートと共に提供されます。この信頼キャッシュにより、ソフトウェアアップデート内のコードのチャンク(**アップデートブレイン**)をプラットフォーム特権で実行できます。アップデートブレインは、ホストシステムがバージョン間で一貫した方法で実行する能力がないソフトウェアアップデートをステージングするための、あらゆる作業を実行します。

Macコンピュータでのペリフェラルプロセッサのセキュリティ

すべての最新のコンピューティングシステムには、ネットワーキング、グラフィックス、電源管理などのタスク専用のペリフェラルプロセッサが多数内蔵されています。これらのペリフェラルプロセッサは多くの場合単一の用途に使用され、プライマリCPUに比べて能力がはるかに劣ります。十分なセキュリティを実装していない内蔵ペリフェラルは、攻撃者がオペレーティングシステムを持続的に感染させることができる、侵害しやすい標的になります。攻撃者は、ペリフェラルプロセッサのファームウェアを感染させることができれば、プライマリCPU上のソフトウェアを標的にでき、機密データを直接取得することさえできます(例えば、暗号化されていないパケットの内容をEthernetデバイスで見ることができます)。

Appleは、可能な限り、必要なペリフェラルプロセッサの数を減らしたり、ファームウェアが必要な設計を回避することに取り組んでいます。それでも独自のファームウェアを含む別個のプロセッサが必要な場合は、攻撃者がそのプロセッサに持続的に侵入できなくするように努めています。これは以下の2つの方法のいずれかでプロセッサを検証することで実行できます:

- 起動時にプライマリCPUから検証済みのファームウェアをダウンロードするようにプロセッサを動作させる
- ペリフェラルプロセッサに専用のセキュアブートチェーンを実装させて、Macが起動するたびにペリフェラルプロセッサのファームウェアを検証するようにする

Appleはベンダーと協力してその実装を監査しベンダーの設計を強化して次のような望ましい特性を含めています:

- 最低限の暗号化強度の確保
- 既知の不正なファームウェアに対する強力な無効化の確保
- デバッグインターフェイスの無効化
- Appleの制御下にあるハードウェアセキュリティモジュール(HSM)に格納されている暗号鍵を使用したファームウェアへの署名

Appleは近年、一部の外部ベンダーと協力して、Appleシリコン用に同じ「Image4」データ構造、検証コード、および署名インフラストラクチャを採用してきました。

ストレージを使用しない操作もストレージとセキュアブートの組み合わせも選択できない場合は、永続ストレージをアップデートする前に暗号化を使ってファームウェアのアップデートに署名し、検証することが必須になります。

Appleシリコン搭載MacのRosetta 2

Appleシリコン搭載Macは、**Rosetta 2**と呼ばれる変換メカニズムを使用してx86_64命令セット用にコンパイルされたコードを実行できます。ジャストインタイムと事前という2種類の変換が用意されています。

ジャストインタイム変換

ジャストインタイム（JIT）変換パイプラインでは、x86_64 Machオブジェクトがイメージ実行パスの早い段階で識別されます。これらのイメージが検出されると、カーネルは制御を動的リンクエディタ（`dyld(1)`）ではなく特殊なRosetta変換スタブに委譲します。そのあと、この変換スタブがイメージの実行中にx86_64ページを変換します。この変換は完全にプロセス内で行われます。カーネルは、ページに障害が発生したときにバイナリに添付されたコード署名に対して各x86_64ページのコードハッシュを検証します。ハッシュの不一致が発生した場合、カーネルはそのプロセスに適した修復ポリシーを適用します。

事前変換

事前（AOT）変換パスでは、システムがそのコードの応答性に最適であると判断した時点で、x86_64バイナリがストレージから読み取られます。変換されたアーティファクトは、特殊なタイプのMachオブジェクトファイルとしてストレージに書き込まれます。そのファイルは実行可能イメージに似ていますが、別のイメージの変換された製品であることを示すためにマークが付けられています。

このモデルでは、AOTアーティファクトは、元のx86_64実行可能イメージからすべてのID情報を導出します。このバインディングを適用するために、特権付きユーザ空間エンティティは、Secure Enclaveによって管理されるデバイス固有の鍵を使用して変換アーティファクトに署名します。この鍵は、制限された資格を使用して特権付きユーザ空間エンティティとして識別される特権付きユーザ空間エンティティにのみ解放されます。変換アーティファクト用に作成されたコードディレクトリには、元のx86_64実行可能イメージのコードディレクトリハッシュが含まれています。変換アーティファクト自体の署名は、**補助的署名**と呼ばれます。

AOTパイプラインはJITパイプラインと同様に開始され、カーネルは動的リンクエディタ（`dyld(1)`）ではなくRosettaランタイムに制御を委譲します。ただし、Rosettaランタイムはプロセス間通信（IPC）クエリをRosettaシステムサービスに送信し、Rosettaシステムサービスが現在の実行可能イメージに使用できるAOT変換があるかどうかを確認します。ある場合、Rosettaサービスはその変換へのハンドルを提供し、それがプロセスにマッピングされて実行されます。実行中にカーネルは、デバイス固有の署名鍵をルートとする署名によって認証される変換アーティファクトのコードディレクトリハッシュを適用します。元のx86_64イメージのコードディレクトリハッシュは、このプロセスには関与しません。

変換されたアーティファクトは、Rosettaサービス以外のエンティティはランタイムにアクセスできないData Vaultに保存されます。Rosettaサービスは、読み取り専用のファイル記述子を個々の変換アーティファクトに配付することにより、キャッシュへのアクセスを管理します。これにより、AOTアーティファクトのキャッシュへのアクセスが制限されます。このサービスのプロセス間通信と依存するフットプリントは、攻撃対象領域を制限するために意図的に非常に狭く保たれています。

元のx86_64イメージのコードディレクトリハッシュがAOT変換アーティファクトの署名にエンコードされたものと一致しない場合、この結果は無効なコード署名と同等であると見なされ、適切な適用アクションが実行されます。

リモートプロセスでカーネルにAOT変換された実行可能ファイルの資格またはその他のコードIDプロパティが照会されると、元のx86_64イメージのIDプロパティがカーネルに返されます。

静的信頼キャッシュの内容

macOS 11以降は、x86_64とarm64のコンピュータコードのスライスを含むMachの「ファット」バイナリと一緒に提供されます。Appleシリコン搭載Macでは、ユーザは、例えばネイティブのarm64バリアントのないプラグインを読み込むために、Rosettaパイプラインを介してシステムバイナリのx86_64スライスを実行することを決定できます。このアプローチをサポートするために、macOSと一緒に提供される静的信頼キャッシュには、一般的に、Machオブジェクトファイルごとに3つのコードディレクトリハッシュが含まれています:

- arm64スライスのコードディレクトリハッシュ
- x86_64スライスのコードディレクトリハッシュ
- x86_64スライスのAOT変換のコードディレクトリハッシュ

RosettaのAOT変換手順は、変換がいつ実行されたか、またはどのデバイスで実行されたかに関係なく、任意の入力に対して同一の出力を再現するという点で決定論的です。

macOSのビルド中に、すべてのMachオブジェクトファイルは、ビルドされているmacOSのバージョンに関連付けられたRosetta AOT変換パイプラインを介して実行され、結果のコードディレクトリハッシュが信頼キャッシュに記録されます。効率のため、実際に変換された製品は、オペレーティングシステムと一緒に提供されず、ユーザが要求したときにオンデマンドで再構成されます。

x86_64イメージがAppleシリコン搭載Macで実行されているときに、そのイメージのコードディレクトリのハッシュが静的信頼キャッシュ内にある場合、結果のAOTアーティファクトのコードディレクトリのハッシュも静的信頼キャッシュにあると予想されます。署名機関はAppleのセキュアブートチェーンのルートであるため、このような製品はデバイス固有の鍵で署名されていません。

無署名のx86_64コード

Appleシリコン搭載Macでは、有効な署名が添付されていない限り、ネイティブのarm64コードを実行することはできません。この署名は、非対称鍵ペアの秘密の半分に基づく実際のIDを持たないアドホックコード署名(`codesign(1)`を参照)と同じくらいシンプルにすることができます(これは単にバイナリの認証されていない測定値です)。

変換されたx86_64コードは、バイナリ互換性のために、署名情報なしでRosettaを介して実行することが許可されています。デバイス固有のSecure Enclave署名手順を介してこのコードに特定のIDが伝達されることはなく、Intelプロセッサ搭載Macで実行されるネイティブの無署名のコードとまったく同じ制限で実行されます。

Macコンピュータでのダイレクトメモリアクセス保護

PCIe、FireWire、Thunderbolt、USBなどの高速インターフェイスで高いスループットを実現するには、コンピュータがペリフェラルからのダイレクトメモリアクセス(DMA)をサポートする必要があります。つまり、CPUが継続的に関与しなくてもRAMの読み出し/書き込みができる必要があります。2012年以降、MacコンピュータはDMAを保護する多くのテクノロジーを実装しているため、あらゆるPCの中で最強かつ最も包括的な一連のDMA保護を備えています。

Appleシリコン搭載Macでのダイレクトメモリアクセス保護

AppleのSystem on Chipには、PCIeポートやThunderboltポートなどのシステム内のDMAエージェントごとにIOMMU(Input/Output Memory Management Unit)が含まれています。各IOMMUにはDMA要求を変換するための独自のアドレス変換テーブルのセットがあるため、PCIeまたはThunderboltで接続されたペリフェラルは、それらを使用するために明示的にマップされているメモリにのみアクセスできます。ペリフェラルは、カーネルやファームウェアなどのシステムのほかの部分に属するメモリやほかのペリフェラルに割り当てられたメモリにはアクセスできません。IOMMUが、使用するようにマップされていないメモリにペリフェラルがアクセスしようとしたことを検出すると、カーネルパニックをトリガします。

Intelプロセッサ搭載Macのダイレクトメモリアクセス保護

Intel Virtualization Technology for Directed I/O（VT-d）を搭載したIntelプロセッサ搭載Macコンピュータは、IOMMUを初期化して、DMAの再マッピングと割り込みの再マッピングをブートプロセスの非常に早い段階で有効にすることで、さまざまなクラスのセキュリティ脆弱性を軽減します。Apple IOMMUハードウェアは、デフォルト拒否ポリシーで操作を開始するため、システムの電源がオンになるとすぐに、自動的にペリフェラルからのDMA要求のブロックが開始されます。ソフトウェアによって初期化されたあと、IOMMUは、使用するように明示的にマップされたメモリ領域への、ペリフェラルからのDMA要求の許可を開始します。

注記: 各IOMMUは独自のペリフェラルのMSIを処理するため、Appleシリコン搭載MacではPCIeの割り込み再マッピングは必要ありません。

macOS 11以降では、Apple T2セキュリティチップを搭載したすべてのMacコンピュータでUEFIドライバが実行され、UEFIドライバが外部デバイスとペアリングされているときに、制限付きのRing 3環境でのDMAを円滑化します。このプロパティは、ブート時に悪質なデバイスがUEFIドライバと予期しない方法で相互作用した場合に発生し得るセキュリティの脆弱性の解消に役立ちます。特に、ドライバでのDMAバッファ処理の脆弱性による影響を軽減します。

macOSのカーネルの安全な拡張

macOS 11以降、他社製のカーネル拡張機能（kext）は、有効になっていてもカーネル内にオンデマンドで読み込むことができません。代わりに、ブートプロセスで読み込まれる**Auxiliary Kernel Collection（AuxKC）**に結合されます。AppleシリコンMacではAuxKCの測定値がLocalPolicyに埋め込まれます（それより前のハードウェアでは、AuxKCはデータボリュームに常駐します）。AuxKCを再構築するには、変更内容をカーネルに読み込むためにユーザの承認とmacOSの再起動が必要であり、セキュアブートが「低セキュリティ」に構成されている必要があります。

重要: macOSでは、kextは推奨されなくなりました。kextはオペレーティングシステムの整合性と信頼性を損なうリスクがあるため、Appleではユーザがカーネルの機能拡張を必要としないソリューションを選択することを推奨しています。

Appleシリコン搭載Macのカーネル拡張機能

Appleシリコン搭載Macでは、kextを明示的に有効にする必要があります。それには、起動時に電源ボタンを押したままにしてOne True Recovery（1TR）モードに入ってから、「低セキュリティ」にダウングレードし、カーネル拡張機能を有効にするチェックボックスをオンにします。このアクションでは、管理者パスワードを入力してダウングレードを承認する必要もあります。1TRとパスワードの要件を組み合わせることで、macOS内部を出発点とするソフトウェアのみの攻撃者が、カーネル権限を取得するために悪用できるkextをmacOSに導入することが困難になります。

ユーザがkextの読み込みを承認すると、上記の「ユーザが承認したカーネル拡張機能の読み込み」のフローを使用してkextのインストールが承認されます。上記のフローで使用される承認は、LocalPolicy内のユーザが承認したkextリスト（UAKL）のSHA384ハッシュをキャプチャするためにも使用されます。そのあとカーネル管理デーモン（`kmd`）が、AuxKCに含める対象としてUAKLで見つかるkextのみの検証を行います。

- システム整合性保護（SIP）が有効になっている場合、各kextの署名はAuxKCに含められる前に検証されます。
- SIPが無効な場合、kextの署名は適用されません。

この方法により、Apple Developer Programに参加していないデベロッパやユーザが、署名される前にkextをテストする「セキュリティ制限なし」のフローを実行できます。

AuxKCが作成されたあと、その測定値がSecure Enclaveに送信されて署名され、起動時にiBootで評価できるImage4データ構造に含められます。AuxKC構造の一部として、kext受信確認も生成されます。この受信確認には実際にAuxKCに含められたkextのリストが含まれます。禁止されているkextが検出された場合に、このセットがUAKLのサブセットになり得るからです。LocalPolicyにはAuxKC Image4データ構造のSHA384ハッシュとkext受信確認が含められます。AuxKC Image4ハッシュは、Secure Enclaveで署名された古いAuxKC Image4ファイルが新しいLocalPolicyで起動できないようにするために、iBootによる起動時の追加検証に使用されます。kext受信確認は、Apple Payなどのサブシステムで、現在読み込まれているkextのいずれかがmacOSの信頼性に干渉する可能性があるかどうかを判断するために使用されます。可能性がある場合は、Apple Pay機能が無効にされることがあります。

システム機能拡張

macOS 10.15では、デベロッパがカーネルレベルではなくユーザ領域内で動作するシステム機能拡張をインストールおよび管理することで、macOSの機能を拡張できるようになっています。システム機能拡張は、ユーザ領域で動作することによってmacOSの信頼性とセキュリティが強化されます。kextは元来オペレーティングシステム全体への完全なアクセス権を持ちますが、ユーザ領域で動作する機能拡張には、指定された機能を実行するために必要な特権のみが付与されます。

デベロッパはDriverKit、EndpointSecurity、NetworkExtensionなどのフレームワークを使用して、USBドライバおよびヒューマンインターフェイスドライバ、エンドポイントセキュリティツール（データ損失防止などのエンドポイントエージェント）、VPNツールおよびネットワークツールを開発できます。いずれの場合も、kextを開発する必要はありません。他社製セキュリティエージェントは、これらのAPIが利用されている場合、またはカーネル拡張機能からそれらのAPIに移行するためのしっかりしたロードマップが定められている場合にのみ使用してください。

ユーザが承認したカーネル拡張機能の読み込み

セキュリティを強化するため、macOS 10.13のインストール時またはインストール後にインストールされたカーネル拡張機能を読み込むには、ユーザの同意が必須になっています。このプロセスを「**ユーザが承認したカーネル拡張機能の読み込み**」と言います。カーネル拡張機能を承認するには、管理者の承認が必要です。以下に該当するカーネル拡張機能の場合は、承認が不要です。

- macOS 10.12以前が実行されているときにMacにインストールされた
- 以前に承認された機能拡張を置き換えるものである
- MacがrecoveryOSからブートした場合に利用可能なspctlコマンドラインツールを使用して、ユーザの同意なしで読み込むことが許可されている
- モバイルデバイス管理（MDM）構成を使用して読み込むことが許可されている

  macOS 10.13.2以降では、ユーザがMDMを使用して、ユーザの同意なしで読み込まれるカーネル拡張機能のリストを指定できます。このオプションを使用するには、macOS 10.13.2を搭載し、Apple School Manager、Apple Business Manager、またはユーザによるMDM登録を介してMDMに登録されているMacが必要です。

macOSのオプションROMのセキュリティ

注記: オプションROMは、現在のところAppleシリコン搭載Macではサポートされていません。

Apple T2セキュリティチップを搭載したMacのオプションROMのセキュリティ

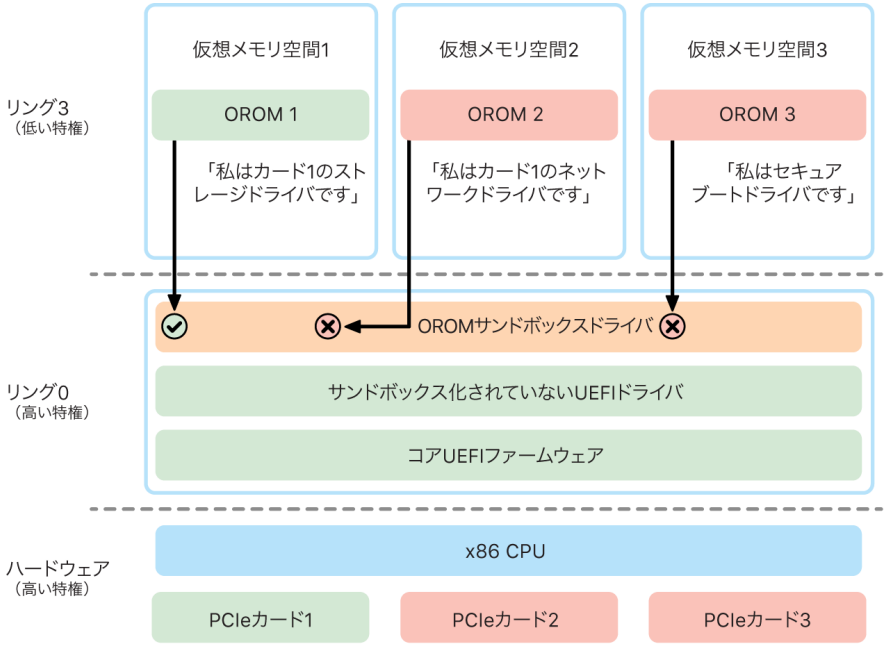
ThunderboltデバイスとPCIeデバイスでは、「オプションROM（OROM）」をデバイスに物理的に接続できます（通常これは真の意味でのROMではなく、ファームウェアが格納される書き換え可能なチップです）。UEFIベースのシステムでは、そのファームウェアは一般にUEFIドライバであり、UEFIファームウェアによって読み込まれ、実行されます。実行されるコードは、そのコードの呼び出し元であるハードウェアを初期化および構成して、残りのファームウェアでそのハードウェアを使用できるようにするためのものです。この機能は、外部RAIDアレイから起動するときなど、ごく初期の起動フェーズで専用の他社製ハードウェアでの読み込みと動作を可能にするために必要です。

ただし、OROMは一般に書き換え可能なため、攻撃者が正当なペリフェラルのOROMを上書きすれば、攻撃者のコードがブートプロセスで早期に実行され、実行環境を改ざんして、あとで読み込まれるソフトウェアの整合性を侵害することができます。同様に、攻撃者が自分の悪質なデバイスをシステムに導入すると、悪質なコードも実行できるようになります。

macOS 10.12.3では、2011年よりあとに販売されたMacコンピュータの動作が変更され、特殊な組み合わせのキーを押さない限り、デフォルトでMacの起動時にOROMが実行されなくなりました。このキーの組み合わせで、不注意によりmacOSのブートシーケンスに悪質なOROMが導入されないように保護されました。ファームウェアパスワードユーティリティのデフォルトの動作も変更され、ユーザがファームウェアパスワードを設定すると、特定のキーの組み合わせを押した場合でもOROMを実行できなくなりました。これにより、Macに物理的にアクセスできる攻撃者によって悪質なOROMが意図的に導入されることを阻止できるようになりました。ファームウェアパスワードを設定していてもOROMを実行する必要があるユーザ向けに、macOSの`firmwarepasswd`コマンドラインツールを使用してデフォルト以外のオプションも構成できます。

OROMサンドボックスのセキュリティ

macOS 10.15では、OROMのサンドボックス化と特権分離のメカニズムを含むように、UEFIファームウェアがアップデートされました。UEFIファームウェアは通常、OROMを含むすべてのコードを、Ring 0と呼ばれる最大CPU特権レベルで実行し、すべてのコードおよびデータ用の単一共有仮想メモリ領域を使用します。Ring 0はmacOSカーネルが実行される権限レベルです。アプリが実行されるのは、それより低い権限レベルのRing 3です。OROMサンドボックスによって、カーネルと同様の仮想メモリ隔離を利用してOROMが特権分離され、OROMがRing 3で実行されるようになりました。



さらに、OROMが呼び出せるインターフェイスが（カーネルでのシステムコールへのフィルタ適用と同様に）制限され、OROMが自らを登録できるデバイスのタイプも（アプリの承認と同様に）制限されています。この設計の利点は、悪質なOROMがRing 0メモリ内にあるどの場所にも直接書き込めなくなることです。代わりに、明確に定義された非常に狭いサンドボックスインターフェイスに限定されます。このインターフェイスの制限によって攻撃対象領域が大幅に縮小され、攻撃者は最初にサンドボックスを回避して特権を昇格せざるを得なくなります。

IntelベースのMacのUEFIファームウェアのセキュリティ

Apple T2セキュリティチップおよびIntelプロセッサ搭載Macは、UEFI（Intel）ファームウェアを使用したセキュリティを備えています。

概要

2006年以降、IntelベースのCPUを搭載したMacコンピュータでは、Extensible Firmware Interface（EFI）開発キット（EDK）バージョン1またはバージョン2に基づくIntel ファームウェアが使用されています。EDK2ベースのコードはUnified Extensible Firmware Interface（UEFI）仕様に準拠しています。このセクションでは、このIntelファームウェアを**UEFIファームウェア**と呼びます。UEFIファームウェアはIntelチップ上で最初に実行されるコードでした。

Apple T2セキュリティチップを搭載していないIntelプロセッサ搭載Macでは、UEFIファームウェアの信頼の起点はそのファームウェアが格納されているチップになります。UEFIファームウェアのアップデートはAppleによってデジタル署名され、ストレージのアップデート前にファームウェアによって検証されます。ロールバック攻撃を防ぐため、アップデートは常に既存のものよりも新しいバージョンである必要があります。ただし、Macに物理的にアクセスできる攻撃者であれば、ハードウェアを使用してファームウェアのストレージチップに接続し、チップをアップデートして悪意あるコンテンツを含めることができる可能性があります。同様に、UEFIファームウェアのブートプロセスの初期（ストレージチップへの書き込み制限より前）に脆弱性が見つかった場合、これもUEFIファームウェアの持続的な感染の原因となる可能性があります。これはIntelプロセッサ搭載ほとんどのPCに共通するハードウェアアーキテクチャの欠点であり、T2チップを搭載していないすべてのIntelプロセッサ搭載Macコンピュータにもこの欠点が存在します。

UEFIファームウェアを破壊する物理的な攻撃を防ぐために、MacコンピュータはT2チップのUEFIファームウェアへの信頼を起点とするように再設計されました。Intelプロセッサ搭載Macのブートプロセスで説明されているように、これらのMacコンピュータでは、UEFIファームウェアの信頼の起点が明確にT2ファームウェアになります。

Intel Management Engine（ME）のサブコンポーネント

UEFIファームウェア内に格納されているサブコンポーネントの1つに、**Intel Management Engine（ME）**ファームウェアがあります。ME（Intelチップ内の個別のプロセッサおよびサブシステム）は、主にIntelベースのグラフィックスのみが搭載されているMacでのオーディオおよびビデオの著作権保護に使用されます。このサブコンポーネントの攻撃対象領域を縮小するため、Intelプロセッサ搭載Macでは、ほとんどのコンポーネントが削除されたカスタムMEファームウェアが実行されます。結果として得られるMac MEファームウェアは、Intelが提供するデフォルトの最小ビルドよりも小さいため、過去にセキュリティ研究者による公開攻撃の対象となっていた多くのコンポーネントは存在しなくなりました。

システム管理モード（SMM）

Intelプロセッサには、通常の動作とは異なる特殊な実行モードがあります。これは**システム管理モード（SMM）**と呼ばれ、当初は電源管理などの時間が重視される動作を処理するために導入されました。ただし、従来Macコンピュータではそのようなアクションに、**システム管理コントローラ（SMC）**というディスクリートマイクロコントローラが使用されてきました。現在はSMCが別個のマイクロコントローラではなくなり、T2チップに内蔵されています。

watchOSのシステムのセキュリティ

Apple Watchは、iOSで使用されるものと同じハードウェアベースのプラットフォームセキュリティ機能の多くを使用します。例えば、Apple Watchは以下の機能を備えています:

- セキュアブートおよび安全なソフトウェアアップデートを実行する
- オペレーティングシステムの整合性を維持する
- デバイス上のデータと、ペアリングされたiPhoneやインターネットとの通信中のデータの両方を保護する

サポートされているテクノロジーには、「システムセキュリティ」に記載されているテクノロジー(KIP、SKP、SCIPなど)のほか、データ保護、キーチェーン、およびネットワークテクノロジーなどがあります。

watchOSをアップデートする

watchOSは夜間にアップデートするように設定できます。アップデート時のApple Watchのパスコードの保存および使用方法について詳しくは、キーバッグを参照してください。

手首検出

手首検出が有効になっている場合は、Apple Watchを手首から外すとすぐに、自動的にロックされます。手首検出が無効になっている場合は、コントロールセンターにApple Watchをロックするためのオプションが表示されます。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Apple Watchアプリを使用します。また、モバイルデバイス管理(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。

アクティベーションロック

iPhoneで「探す」をオンにすると、ペアリングされているApple Watchでもアクティベーションロックを使用できます。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。

iPhoneとの安全なペアリング

Apple Watchは、一度に1台のiPhoneとのみペアリングできます。Apple Watchのペアリングが解除されると、iPhoneは、Watchからすべてのコンテンツとデータを消去するよう指示します。

Apple WatchとiPhoneとのペアリングは、公開鍵を交換する帯域外プロセスと、その直後のBluetooth® Low Energy（BLE）リンク共有シークレットを使って安全が確保されます。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。

BLEセッションが確立され、Bluetoothコア仕様で使用可能な最高のセキュリティプロトコルを使用して暗号化されたあと、iPhoneとApple Watchが以下のいずれかを使用して鍵を交換します:

- iMessageのセキュリティの概要で説明されている、Apple Identity Service（IDS）から応用されたプロセス。
- IKEv2/IPsecを使用した鍵交換。最初の鍵交換はBluetoothセッション鍵（ペアリングの場合）またはIDS鍵（オペレーティングシステムのアップデートの場合）を使用して認証されます。各デバイスでランダムな256ビットのEd25519公開/秘密鍵ペアが生成され、最初の鍵交換プロセスで公開鍵が交換されます。watchOS 10以降を搭載したApple Watchが初めてペアリングされたとき、秘密鍵はそのSecure Enclaveをルートとします。

  iOS 17以降を搭載したiPhoneでは、秘密鍵はSecure Enclaveをルートにしません。iCloudバックアップを同じiPhoneに復元するユーザは、移行しなくても既存のApple Watchのペアリングを保持するためです。

注記: 鍵交換と暗号化に使用されるメカニズムは、iPhoneおよびApple Watchのオペレーティングシステムのバージョンによって異なります。iOS 13以降を搭載したiPhoneデバイスは、watchOS 6以降を搭載したApple Watchとペアリングされた場合、鍵交換と暗号化にIKEv2/IPsecのみが使用されます。

鍵の交換後に、以下のことが行われます:

- Bluetoothセッション鍵が破棄され、iPhoneとApple Watch間のすべての通信が、上記のいずれかの方法で暗号化されます。暗号化されたBluetooth、Wi-Fi、およびモバイルデータ通信のリンクが二次的な暗号化レイヤーを提供します。
- （IKEv2/IPsecのみ）鍵がシステムキーチェーンに保存され、デバイス間での今後のIKEv2/IPsecセッションの認証に使用されます。これらのデバイス間でそれ以降行われる通信は、watchOS 8以降を搭載したApple Watch Series 4以降とペアリングされているiOS 15以降を搭載したiPhoneデバイスでは、AES-256-GCMを使用して暗号化され、整合性が保護されます。（256ビット鍵によるChaCha20-Poly1305は、古いデバイスまたは古いバージョンのオペレーティングシステムを搭載したデバイスで使用されます。）

だれかが持続的な識別情報をブロードキャストした場合にデバイスがローカルでトラッキングされるリスクを減らすため、Bluetooth Low Energyデバイスのアドレスは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アプリをサポートするため、FaceTimeのセキュリティで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Apple Identity Service（IDS）、または直接のインターネット接続が使用されます。

Apple Watchは、ハードウェアで暗号化されたストレージと、ファイルおよびキーチェーン項目のクラスベースの保護を実装しています。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。詳しくは、データ保護用のキーバッグを参照してください。

自動ロック解除とApple Watch

複数のAppleデバイスを使用する場合の利便性を高めるため、特定の状況下では一部のデバイスでほかのデバイスのロックを自動的に解除できます。自動ロック解除は3つの使用方法をサポートしています:

- iPhoneでApple Watchのロックを解除できます。
- Apple WatchでMacのロックを解除できます。
- ユーザが鼻と口を覆った状態で検出された場合、Apple WatchでiPhoneのロックを解除できます。

3つの使用方法はすべて、相互に認証されたStation-to-Station(STS)プロトコルという同じ基盤の上に構築されています。このプロトコルでは、機能が有効になったときに長期鍵が交換され、リクエストごとに一時的な一意のセッション鍵がネゴシエートされます。基盤となる通信チャネルにかかわらず、STSトンネルは両方のデバイスのSecure Enclave間で直接ネゴシエートされ、すべての暗号化要素が安全なドメイン内にとどまります(ただしSecure Enclaveを搭載していないMacコンピュータは例外で、STSトンネルの終点がカーネル内になります)。

ロック解除

ロック解除シーケンスは、全体を2段階に分けることができます。最初に、ロック解除されるデバイス(「ターゲット」)が暗号ロック解除シークレットを生成し、ロック解除を実行するデバイス(「イニシエータ」)に送信します。イニシエータはその後、以前に生成されたシークレットを使用してロック解除を実行します。

自動ロック解除が可能な状態にするため、両方のデバイスがBLE接続を使用して接続されます。次に、ターゲットデバイスによってランダムに生成された32バイトのロック解除シークレットがSTSトンネル経由でイニシエータに送信されます。生体認証またはパスコードによる次回のロック解除時に、ターゲットデバイスがそのパスコードから導出された鍵(PDK)をロック解除シークレットでラップし、メモリ内のロック解除シークレットを破棄します。

ロック解除を実行するため、デバイスが新しいBLE接続を開始してから、ピアツーピアWi-Fiを使用して互いのおよその距離を安全に取得します。デバイスが指定された範囲内にあり、必要なセキュリティポリシーに適合していれば、イニシエータがロック解除シークレットをSTSトンネル経由でターゲットに送信します。その後、ターゲットが32バイトの新しいロック解除シークレットを生成し、イニシエータに返します。イニシエータによって送信された最新のロック解除シークレットでロック解除レコードが正常に復号されると、ターゲットデバイスのロックが解除され、PDKが新しいロック解除シークレットで再ラップされます。最後に、ターゲットのメモリ内の新しいロック解除シークレットとPDKが破棄されます。

Apple Watchの自動ロック解除のセキュリティポリシー

利便性を高めるため、Apple Watchの最初の起動の直後から、ユーザがApple Watch自体でパスコードを入力しなくてもiPhoneでロックを解除できます。そのために、ランダムなロック解除シークレット(この機能を有効にしたあとの初回のロック解除シーケンスで生成されます)を使用して長期エスクローレコードが作成され、Apple Watchのキーバッグに保存されます。このエスクローレコードのシークレットがiPhoneのキーチェーンに保存され、Apple Watchが再起動されるたびに、その後の新しいセッションをブートストラップするために使用されます。

iPhoneの自動ロック解除のセキュリティポリシー

Apple WatchでのiPhoneの自動ロック解除には、追加のセキュリティポリシーが適用されます。Apple Payやアプリの承認などのその他の操作では、Apple WatchをiPhoneのFace IDの代わりに使用することはできません。Apple Watchがペアリングされているi Phoneのロック解除に成功すると、Apple Watchに通知が表示され、関連付けられた触覚が再生されます。通知にある「iPhoneをロック」ボタンをユーザがタップすると、Apple WatchがBLE経由でiPhoneにロックコマンドを送信します。iPhoneはロックコマンドを受信するとロックされ、Face IDと、Apple Watchでのロック解除の両方を無効にします。次回のiPhoneのロック解除は、iPhoneのパスコードで行う必要があります。

ペアリングされているiPhoneのApple Watchからのロック解除（有効な場合）を正常に行うには、以下の基準を満たす必要があります:

- 関連付けられたApple Watchが手首に装着され、ロックが解除されたあと、iPhoneのロックが別の方法で1回以上解除されている必要があります。
- 鼻と口が覆われていることをセンサーが検知できる必要があります。
- 測定された距離が2 ~ 3m以内である必要があります。
- Apple Watchが睡眠モードでない必要があります。
- Apple WatchまたはiPhoneのロックが最近解除されているか、装着している人がアクティブである（睡眠中でないなど）ことを示す物理的な動きをApple Watchが感知している必要があります。
- iPhoneのロックが過去6.5時間以内に1回以上解除されている必要があります。
- iPhoneが、Face IDによるデバイスのロック解除の実行が許可された状態である必要があります。（詳しくは、Face ID、Touch ID、パスコード、パスワードを参照してください。）

macOSでApple Watchを使って承認する

Apple Watchでの自動ロック解除が有効になっている場合、Apple WatchをTouch IDの代わりに使用するか、Touch IDと併用して、以下のものからの許可および認証の要求を承認できます。

- 承認を要求するmacOSおよびAppleアプリ
- 認証を要求する他社製アプリ
- 保存されているSafariパスワード
- 秘密メモ

Wi-Fi、モバイルデータ通信、iCloud、およびGmailの安全な使用

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、自動的に接続します。この自動接続の動作は、接続後、Apple Watchの設定アプリの「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の設定アプリの「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アプリの「メール」セクションでGoogleへの認証を行う必要があります。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できるようになります。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。

乱数の生成

暗号擬似乱数ジェネレータ(CPRNG)は安全なソフトウェアの重要な構成要素です。安全なソフトウェアを実現するために、AppleはiOS、iPadOS、macOS、tvOS、およびwatchOSカーネルで実行する、信頼性の高いソフトウェアCPRNGを提供しています。CPRNGはシステムから生のエントロピーを集め、カーネルとユーザ空間の両方でコンシューマに安全な乱数を提供するという役割を担います。

エントロピーソース

カーネルのCPRNGは、起動時とデバイスのライフタイム全体を通じて、複数のエントロピーソースからシード値を得ます。エントロピーソースには以下が含まれます(使用できる場合):

- Secure EnclaveのハードウェアTRNG
- 起動時に収集された、タイミングベースのジッタ
- ハードウェア割り込みから収集されたエントロピー
- 起動をまたいでエントロピーを保持するために使用するシードファイル
- Intelの乱数命令 — RDSEEDやRDRANDなど(Intelプロセッサ搭載Macのみ)

カーネルCPRNG

カーネルのCPRNGはFortuna由来の設計で、256ビットのセキュリティレベルを対象としています。カーネルのCPRNGは以下のAPIを使用してユーザ空間のコンシューマに高品質な乱数を提供します:

- `getentropy`(2)システム呼び出し
- ランダムデバイス(/dev/random)

カーネルのCPRNGは、ランダムデバイスへの書き込みを通じて、ユーザが提供したエントロピーを受け入れます。

Apple Security Research Device

Apple Security Research Deviceは、セキュリティ研究者がiPhoneのプラットフォームセキュリティ機能を停止したり無効にしたりしなくてもiOSに関する研究を実行できるように、特別に融合されたiPhoneです。このデバイスを使用すると、研究者はプラットフォームと同等の権限で実行されるコンテンツをサイドロードできるため、実稼働デバイスのコンテンツをより厳密にモデル化したプラットフォームで研究を行うことができます。

ユーザデバイスがセキュリティ研究用デバイスの実行ポリシーの影響を受けないようにするために、ポリシーの変更はiBootとブートカーネルコレクションのバリアントに実装されています。これらはユーザのハードウェアではブートに失敗します。研究用iBootは、新しい融合状態をチェックし、研究用以外の融合されたハードウェアで実行されている場合はパニックループに入ります。

cryptexサブシステムを使用すると、研究者は、パーソナライズされた信頼キャッシュと、対応するコンテンツを含むディスクイメージを読み込むことができます。このサブシステムがユーザデバイスでの実行を許可しないようにするための徹底した防御対策が数多く実装されています:

- `launchd`は、通常の顧客用デバイスを検出した場合には`cryptexd`のlaunchdプロパティリストを読み込みません。
- `cryptexd`は、通常の顧客用デバイスを検出した場合には中断します。
- `AppleImage4`からは、通常の顧客用デバイスで研究用cryptexを検証するために使用されるアンチリプレイ値は得られません。
- 署名サーバは、明示的な許可リストにないデバイスのcryptexディスクイメージをパーソナライズすることを拒否します。

セキュリティ研究者のプライバシーを尊重するために、実行可能ファイルまたはカーネルキャッシュの測定値(ハッシュなど)とセキュリティ研究用デバイスの識別子のみが、パーソナライズ中にAppleに送信されます。Appleは、デバイスに読み込まれているcryptexのコンテンツを受信しません。

悪意のある第三者が研究用デバイスをユーザデバイスに見せかけて、ターゲットをだまして日常の用途のために使用させようとするのを回避するために、セキュリティ研究用デバイスには以下の違いがあります:

- セキュリティ研究用デバイスは、充電中しか起動しません。充電には、LightningケーブルまたはQi互換の充電器を使用することができます。起動時にデバイスが充電されていない場合、デバイスはリカバリモードに入ります。ユーザが充電を開始してデバイスを再起動すると、通常通り起動します。XNUが起動するとすぐに、操作を続けるためにデバイスを充電する必要がなくなります。
- iBootの起動時に、Appleロゴの下に「**Security Research Device**」という単語が表示されます。
- XNUカーネルは冗長モードでブートします。
- デバイスの側面にメッセージがエッチングされています。"Property of Apple. Confidential and Proprietary.Call +1 877 595 1125."

以下は、ブート後に出現するソフトウェアに実装されている追加の対策です。

- デバイスのセットアップ中に「**Security Research Device**」という単語が表示されます。
- ロック画面と設定アプリに「**Security Research Device**」という単語が表示されます。

セキュリティ研究用デバイスは、ユーザデバイスにはない次の機能を研究者に提供します。研究者は次のことができます:

- Appleオペレーティングシステムのコンポーネントと同じアクセス許可レベルで任意の資格を持つデバイスに、実行可能コードをサイドロードする
- 起動時にサービスを開始する
- 再起動後もコンテンツを保持する
- `research.com.apple.license-to-operate`資格を使用して、あるプロセスが、システムプロセスを含むシステム上のほかのプロセスをデバッグすることを許可する。

  `research.`名前空間は、AppleMobileFileIntegrityカーネル拡張機能のRESEARCHバリアントでのみ尊重されます。この資格を持つプロセスは、顧客用デバイスでは署名の検証中に終了されます。
- カスタムカーネルキャッシュをパーソナライズして復元する

暗号化とデータ保護

暗号化とデータ保護の概要

セキュアブートチェーン、システムのセキュリティ、アプリのセキュリティはすべて、信頼されたコードとアプリのみをデバイスで実行するために有効な機能です。デバイスを紛失したり、信頼されていないコードを実行するなど、セキュリティインフラストラクチャのほかの部分が侵害された場合でも、Appleデバイスはユーザデータを保護するための暗号化機能を搭載しています。これらすべての機能により、個人や企業の情報が保護されるほか、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管理者の双方がメリットを得ることができます。

iPhoneおよびiPadデバイスでは、「**データ保護**」と呼ばれるファイル暗号化方式が使用されます。一方、Intelプロセッサ搭載Macでは、「**FileVault**」と呼ばれるボリューム暗号化技術によってデータが保護されます。Appleシリコン搭載Macは、データ保護をサポートするハイブリッドモデルを採用しており、これには2つの注意点があります。最も低い保護レベル（クラスD）はサポートされません。また、デフォルトのレベル（クラスC）はボリュームキーを使用し、Intelプロセッサ搭載MacでのFileVaultと同じように動作します。いずれの場合も、鍵管理階層はSecure Enclaveの専用シリコンと、高速な暗号化をサポートする専用のAESエンジンに基づき、侵害を受けるリスクがあるカーネルオペレーティングシステムやCPUに存続期間の長い暗号鍵が公開されない仕組みを確立しています。（Intelプロセッサ搭載Macのうち、T1チップを搭載しているものやSecure Enclaveを搭載していないものでは、FileVault暗号鍵を保護するために専用シリコンは使用されません。）

データ保護とFileVaultを使用してデータへの不正アクセスを防止するだけでなく、Appleの**オペレーティングシステムのカーネル**によって保護機能とセキュリティ機能が適用されます。カーネルは、サンドボックス化したアプリのアクセス制御と（これによってアプリがアクセスできるデータが制限されます）、**Data Vault**と呼ばれるメカニズム（アプリによる呼び出しを制限する代わりに、アプリのデータに対するその他のアプリからのアクセスを制限します）も使用します。

パスコードとパスワード

ユーザデータを悪意ある攻撃から保護するために、AppleはiOSとiPadOSでパスコード、macOSでパスワードを使用しています。パスコードまたはパスワードは長いほど強力であり、総当たり（ブルートフォース）攻撃を抑制しやすくなります。攻撃をさらに抑制するために、Appleは待ち時間を適用したり（iOSとiPadOSの場合）、パスワードの入力試行の回数を制限したりしています（Macの場合）。

iOSとiPadOSでは、ユーザがデバイスパスコードまたはパスワードを設定することで、データ保護が自動的に有効になります。データ保護は、Appleシリコン搭載Mac、Apple TV、Apple WatchなどのAppleシステムオンチップ（SoC）を搭載したほかのデバイスでも有効になっています。macOSでは、Appleは組み込まれたボリューム暗号化プログラムである**FileVault**を使用します。

強力なパスコードとパスワードでセキュリティが強化される仕組み

iOSとiPadOS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に対応しています。パスコードまたはパスワードを設定すると、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。

パスコードまたはパスワードはデバイスの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、英字の小文字と数字を使った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。

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。また、Face IDやTouch IDを使用すれば、入力するには実用的でない長さのパスコードも設定しやすくなります。強力なパスコードを使うことで、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、1日に何度も実行するデバイスのロック解除のユーザ体験が損なわれることもありません。

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。

ユーザが「設定」>「Touch IDとパスコード」または「Face IDとパスコード」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。

待ち時間の延長によって総当たり（ブルートフォース）攻撃を抑制する仕組み

iOS、iPadOS、およびmacOSでは、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、無効なパスコード、パスワード、またはPIN（デバイスとデバイスの状態に応じて）が入力された場合、次の入力までの待ち時間が以下の表の通りに延長されます。

試行回数	3	4	5	6	7	8	9	10回以上
iOSおよびiPadOSのロック画面	なし	1分	5分	15分	1時間	3時間	8時間	デバイスは無効になっていて、MacまたはPCに接続する必要があります
watchOSのロック画面	なし	1分	5分	15分	1時間	3時間	8時間	デバイスは無効になっていて、iPhoneに接続する必要があります
macOSのログインウインドウとロック画面	なし	1分	5分	15分	1時間	3時間	8時間	8時間
macOSリカバリモード	なし	1分	5分	15分	1時間	3時間	8時間	以下の「macOSで待ち時間の延長によって総当たり（ブルートフォース）攻撃を抑制する仕組み」を参照

試行回数	3	4	5	6	7	8	9	10回以上
FileVaultと復旧キー (個人、組織、またはiCloud)	なし	1分	5分	15分	1時間	3時間	8時間	以下の「macOSで待ち時間の延長によって総当たり(ブルートフォース)攻撃を抑制する仕組み」を参照
macOSのリモートロックのPINコード	1分	5分	15分	30分	1時間	1時間	1時間	1時間

iPhoneまたはiPadで「データを消去」オプション(「設定」>「[Face ID]とパスコード」または「[Touch ID]とパスコード」)をオンにした場合、誤ったパスコードが10回連続で入力されると、ストレージからすべてのコンテンツと設定が削除されます。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、この機能に対応するモバイルデバイス管理(MDM)ソリューションおよびMicrosoft 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によって待ち時間が強制的に適用されます。待ち時間が適用されているデバイスを再起動しても待ち時間は適用されたまま、同じ期間の待ち時間がカウントされます。

macOSで待ち時間の延長によって総当たり(ブルートフォース)攻撃を抑制する仕組み

総当たり(ブルートフォース)攻撃を防ぐために、Mac起動時のログインウインドウでは、パスワードの入力試行が連続10回までに制限され、パスワードを一定の回数間違えると、次に入力できるまでの待ち時間が長くなります。待ち時間はSecure Enclaveによって適用されます。待ち時間が適用されているMacを再起動しても待ち時間は適用されたままで、同じ期間の待ち時間が最初からカウントされます。

マルウェアがユーザのパスワードの入力試行を続けることでデータが完全に失われるのを避けるため、ユーザがMacへのログインに成功したあとはこれらの制限は適用されなくなりますが、再起動後は再び適用されます。10回の試行回数に達すると、recoveryOSが再起動して、さらに10回の試行が可能になります。その回数にも達すると、FileVaultリカバリメカニズム(iCloud復元、FileVault復旧キー、組織のキー)ごとにさらに10回の試行、つまり最大30回の試行が可能になります。これらの回数にも達すると、Secure Enclaveでは、ボリュームの復号またはパスワードの検証要求が一切処理されなくなり、ドライブ上のデータは復元不可能になります。

エンタープライズ環境では、データを保護するために、IT部門がMDMソリューションを使用してFileVaultの構成ポリシーを定義し、適用することが推奨されます。組織の場合、暗号化されたボリュームの管理方法には、組織の復旧キー、個人の復旧キー(任意でMDMに保存してエスクロー可能)、その両方の組み合わせなど、複数のオプションがあります。復旧キーのローテーションをMDMのポリシーとして設定することもできます。

Apple T2セキュリティチップを搭載したMacでは、パスワードはほぼ同じ機能を果たします。ただし、生成される鍵は、データ保護ではなくFileVault暗号化に使用されます。また、macOSでは、以下の追加のパスワードリカバリオプションを使用できます。

- iCloud復元
- FileVault復旧
- FileVaultの組織のキー

データ保護

データ保護の概要

iPhone、iPad、Apple Watch、Apple TV、AppleシリコンMacなどのApple SoCを搭載したデバイスでは、デバイスのフラッシュストレージに保存されたデータを保護するために、「データ保護」と呼ばれる技術が使用されます。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と同時に、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。一部のシステムアプリ(「メッセージ」、「メール」、「カレンダー」、「連絡先」、「写真」など)とヘルスケアデータの値は、デフォルトでデータ保護を使用します。他社製アプリにもこの保護は自動で適用されます。

実装

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、Appleデバイスに内蔵されたハードウェア暗号化技術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。また、APFS(Apple File System)によって、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。

データボリューム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。ハードウェアAESエンジンは、ファイルがフラッシュストレージに書き込まれるときに、その鍵を使用してファイルを暗号化します。A14 ~ A17およびM1 ~ M3を搭載したデバイスでは、暗号化にXTSモードのAES-256が使用され、256ビット鍵(Per Fileキー)が鍵導出関数(NIST Special Publication 800-108)で処理されることにより、256ビットの調整鍵と256ビットの暗号鍵が導出されます。A9 ~ A13およびS5 ~ S9を搭載したデバイスでは、暗号化にXTSモードのAES-128が使用され、256ビットのPer Fileキーが128ビットの調整鍵と128ビットの暗号鍵に分割されています。

AppleシリコンMacでは、データ保護はデフォルトでクラスCになっていますが(データ保護クラスを参照してください)、Per ExtentキーやPer Fileキーではなくボリュームキーが使用されます。これにより事実上、FileVaultでユーザデータを保護する場合と同じセキュリティモデルが再現されます。ただし、パスワードを暗号鍵の階層とタングルして完全な保護を受けるには、ユーザがFileVaultを有効にする必要があります。デベロッパは、Per FileまたはPer Extentキーを使用するさらに高レベルの保護クラスを選択することもできます。

Appleデバイスのデータ保護

データ保護をサポートするAppleデバイスでは、各ファイルが一意のPer File(またはPer Extent)キーで保護されます。これらのキーはNIST AED鍵ラップアルゴリズムでラップされますが、さらにファイルアクセスの方法に応じて、複数あるクラスキーのいずれかでラップされます。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。

APFSフォーマット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。そしてフラッシュストレージ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。

データボリュームのファイルシステム内にあるすべてのファイルのメタデータは、ランダムなボリュームキーで暗号化されます。このキーは、オペレーティングシステムが初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。ボリュームキーは、長期保存のために、Secure Enclaveのみが知るキーラッピング鍵によって暗号化およびラッピングされます。キーラッピング鍵は、ユーザがデバイスを消去するたびに変更されます。A9以降のSoCのSecure Enclaveでは、アンチリプレイシステムに基づくエントロピーによって、消去可能性が実現され、保有するアセット、中でも特にキーラッピング鍵が保護されます。詳しくは、セキュア不揮発性ストレージを参照してください。

Per FileまたはPer Extentキーと同様に、データボリュームの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鍵が保存されると、さらにEffaceable Storageに保存された「消去可能鍵」またはメディアキーラッピング鍵を使用してラッピングされ、Secure Enclaveアンチリプレイメカニズムによって保護されます。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、要求に応じて素早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モバイルデバイス管理(MDM)ソリューション、Microsoft 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、優れた柔軟性と高いパフォーマンスの両方を実現しています。例えば、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。

データ保護クラス

データ保護がサポートされる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アプリ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。Appleシリコン搭載Macコンピュータでは、Class D: No Protectionには対応しません。また、ログインおよびログアウトの前後ではセキュリティ境界が確立されます(iPhoneおよびiPadとは異なり、ロックおよびロック解除の前後では確立されません)。

クラス	保護タイプ
Class A: Complete Protection	NSFileProtectionComplete
Class B: Protected Unless Open	NSFileProtectionCompleteUnlessOpen
Class C: Protected Until First User Authentication **注記:** macOSでのFileVault保護特性の再作成にはボリュームキーが使用されます。	NSFileProtectionCompleteUntilFirstUserAuthentication
Class D: No Protection **注記:** macOSではサポートされていません。	NSFileProtectionNone

Complete Protection

NSFileProtectionComplete: クラスキーは、ユーザのパスコードまたはパスワードとデバイスの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Face IDまたはTouch IDでデバイスをロック解除(ログイン)しない限りアクセスできなくなります。

macOSでは、最後のユーザがログアウトした直後、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でデバイスにログイン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、デバイスがロックされているときまたはユーザがログインしていないとき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、非対称楕円曲線暗号方式（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。鍵導出関数は、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。SHA256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。

macOSでは、NSFileProtectionCompleteUnlessOpenのプライベート部分は、システム上のいずれかのユーザがログインまたは認証されている限りアクセスできます。

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またはユーザのログアウト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。すべての他社製アプリでは、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。

macOSでは、このクラスはボリュームがマウントされている限りアクセスできるボリュームキーを使用し、FileVaultと同様に動作します。

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デバイスやiPadOS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。

macOSではサポートされていません。

注記: ブートされたオペレーティングシステムに対応しないmacOSのボリュームでは、ボリュームがマウントされている限りすべてのデータ保護クラスにアクセスできます。デフォルトのデータ保護クラスはNSFileProtectionCompleteUntilFirstUserAuthenticationです。エクステントごとの鍵機能はRosetta 2とネイティブアプリの両方で使用できます。

データ保護用のキーバッグ

iOS、iPadOS、tvOS、およびwatchOSでは、ファイルとキーチェーンの両方のデータ保護クラスの鍵がキーバッグに収集されて管理されます。これらのオペレーティングシステムで使用されるキーバッグは、ユーザ、デバイス、バックアップ、エスクロー、およびiCloudバックアップです。

ユーザキーバッグ

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。例えば、パスコードが入力されると、NSFileProtectionComplete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)ファイルです。

A9より前のSoCを搭載したデバイスでは、この.plistファイルの内容は、Effaceable Storageに保存された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。

A9以降のSoCを搭載したデバイスでは、この.plistファイルに、Secure Enclaveが制御するアンチリプレイ値によって保護されたロッカーにキーバッグが保存されていることを示す鍵が含まれます。

ユーザキーバッグはSecure Enclaveが管理しており、デバイスのロック状態に関してはSecure Enclave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、デバイスがロック解除されていると報告されます。

デバイスキーバッグ

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、ラップされているクラスキーの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iPadOS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とiPadOSでは、ユーザごとのファイルシステムコンテンツを個別に暗号化することがサポートされていないため、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iPhoneデバイスやiPad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

バックアップキーバッグは、Finder(macOS 10.15以降)またはiTunes(macOS 10.14以前)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。

設定したパスワードで保護されたこのキーバッグに、鍵導出関数PBKDF2が1000万回反復して適用されます。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

エスクローキーバッグは、USB経由でのFinder（macOS 10.15以降）またはiTunes（macOS 10.14以前）との同期と、モバイルデバイス管理（MDM）で使用されます。このキーバッグにより、Finderまたは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、Finderまたは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初めてFinderまたは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初めてFinderまたは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 UIDから導出された鍵で暗号化されます。

A9以降のSoCでは、ワンタイムロック解除トークンはカウンタやEffaceable Storageに依存しなくなりました。代わりに、Secure Enclaveが制御するアンチリプレイ値によって保護されています。

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。iOS 13以降とiPadOS 13.1以降では、このトークンは、Secure Enclaveによって保護されたロッカーに保存されます。iOS 13より前では、このトークンはSecure Enclaveから書き出され、Effaceable Storageに書き込まれました。または、Secure Enclaveのアンチリプレイメカニズムによって保護されました。デバイスが20分以内に再起動しなかった場合は、ポリシータイマーによってカウンタが増分されました。

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以降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

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です（Protected Unless Openデータ保護クラスと同様にCurve25519を使用）。iCloudキーチェーンの復元でのバックアップキーチェーンを保護するのにも、非対称キーバッグが使用されます。

代替起動モードでの鍵の保護

データ保護は、認証に成功したあと、認証されたユーザのみがユーザデータにアクセスできるように設計されています。データ保護クラスはさまざまなユースケースをサポートするように設計されています。例えば、デバイスが一度ロック解除されたあとであれば、ロックされていてもデータの読み込みと書き込みができる機能があります。代替起動モードでのユーザデータへのアクセスを保護するためには、その他の手段も使用されます。これには、デバイスファームウェアアップデート(DFU)モード、リカバリモード、Apple Diagnostics、さらにはソフトウェアアップデート中に使用される手段までが含まれます。これらの機能の基礎にあるのはハードウェアとソフトウェアの機能を組み合わせたものであり、Appleが設計したシリコンの進化に伴って拡張されてきました。

機能	A10	A11–A17 S3–S9 M1、M2、M3
リカバリ: すべてのデータ保護クラスを保護	✓	✓
DFUモード、リカバリ、ソフトウェアアップデートの代替起動: クラスA、クラスB、クラスCデータ保護	✗	✓

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、鍵導出関数にこれらのシードビットが埋め込まれます。シードビットの使われ方はSystem on Chipによって異なります:

- 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キーなど)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キーなど)では設定されません。
- iOS 13以降とiPadOS 13.1以降では、A10以降を搭載したデバイスの場合、診断モードで起動するとすべてのユーザデータが暗号化によってアクセス不能になります。この仕組みを実現するために、メディア鍵へのアクセス可否を設定する追加のシードビットが使用されます。データ保護機能によって暗号化されたデータボリューム上のメタデータ(とすべてのファイルのコンテンツ)にアクセスするには、このメディア鍵が必要です。この保護機能では、ユーザのパスコードが必要なクラスだけでなく、すべてのクラス(A、B、C、D)で保護されたファイルが対象になります。
- A12 SoCでは、アプリケーションプロセッサがデバイスファームウェアアップグレード(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ます。これは、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ためです。

デバイスをDFUモードにしたあと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。

デバイスをDFUモードにする方法については、Appleの以下のサポート記事を参照してください。

デバイス	Appleサポートの記事
iPhone、iPad	iPhoneのパスコードを忘れた場合
Apple TV	Apple TVに警告シンボルが表示される場合
Appleシリコン搭載Mac	Macのファームウェアを復活させる/復元する方法

攻撃を受けたときのユーザデータ保護

多くの場合、ユーザデータを抜き出そうとする攻撃者は数多くのテクニックを試します。例えば、暗号化されたデータを他の媒体に抜き出して総当たり(ブルートフォース)攻撃を加えたり、オペレーティングシステムのバージョンの改ざんや、デバイスのセキュリティポリシーの変更や弱体化によって攻撃を容易にするといったものです。デバイス上のデータを攻撃するには、多くの場合、Thunderbolt、Lightning、USB-Cなどの物理インターフェイスを使用してデバイスと通信する必要があります。Appleデバイスには、そのような攻撃を防ぐための機能が用意されています。

Appleデバイスでは「**シールドキー保護(SKP)**」と呼ばれるテクノロジーがサポートされています。このテクノロジーは、暗号化要素がデバイス外に出された場合や、オペレーティングシステムのバージョンやセキュリティ設定が適切なユーザ承認を経ずに改ざんされた場合に、暗号化要素を利用できなくするように設計されています。この機能はSecure Enclaveが提供するものではなく、代わりにより低層に存在するハードウェアレジスタが対応します。これは、Secure Enclaveに依存しないユーザデータの復号に必要な鍵の保護層を追加するためです。

注記: SKPはAppleが設計したSoCを搭載したデバイスでのみ利用できます。

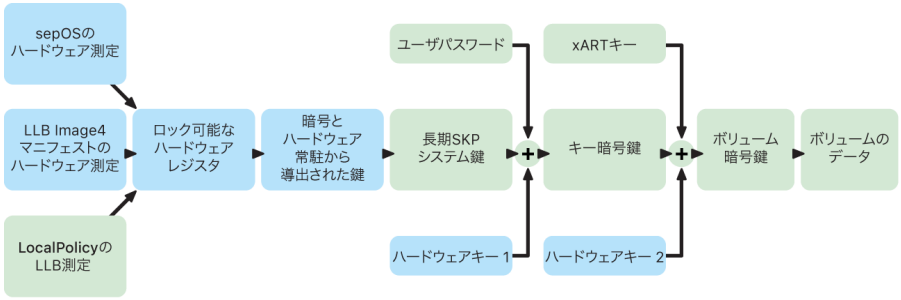
機能	A11–A17 S3–S9 M1、M2、M3
シールドキー保護	✓

iPhoneデバイスとiPadデバイスは、承認された所有者がデバイスを物理的に管理している可能性が高い状況においてのみ、データ接続が有効になるように構成することもできます。

シールドキー保護(SKP)

データ保護をサポートするAppleデバイスでは、キー暗号鍵(KEK)はシステム上のソフトウェアの測定によって保護(または封印)され、Secure Enclaveからのみ利用可能なUIDに関連付けられます。Appleシリコン搭載Macでは、システム上のセキュリティポリシーに関する情報を取り込むことで、KEKの保護がさらに強化されています。これは、ほかのプラットフォームではサポートされない重要なセキュリティポリシーの変更(セキュアブートやSIPの無効化など)がmacOSではサポートされているためです。Appleシリコン搭載Macでは、この保護の対象にはFileVaultの鍵も含まれます。これは、FileVaultはデータ保護(クラスC)を使用して実装されているためです。

ユーザパスワード、長期SKP鍵、およびハードウェア鍵1(Secure EnclaveのUID)をタングルして生成される鍵を、「**パスワードから導出された鍵**」といいます。この鍵は、ユーザのキーバッグ(サポートされるすべてのプラットフォーム)およびKEK(macOSのみ)を保護し、生体認証でのロック解除やApple Watchなどのほかのデバイスでの自動ロック解除を可能にするために使用されます。



Secure Enclave Bootモニタは読み込まれたSecure Enclave OSの測定値を取得します。アプリケーションプロセッサのBoot ROMがLLBに付属したImage4マニフェストを測定するとき、そのマニフェストには、システムとペアリングされたその他のファームウェアのうち、読み込まれたものすべての測定値も含まれています。LocalPolicyには読み込まれたmacOSのコアセキュリティ構成が含まれます。LocalPolicyにはmacOS Image4マニフェストのハッシュである`nsih`フィールドも含まれます。macOS Image4マニフェストには、macOSとペアリングされたすべてのファームウェアの測定値、およびブートカーネルコレクションや署名済みシステムボリューム（SSV）のルートハッシュなどのコアmacOSブートオブジェクトの測定値が含まれます。

攻撃者が予期せず上記の測定されたファームウェア、ソフトウェア、またはセキュリティ構成コンポーネントのいずれかを変更できた場合には、それによりハードウェアレジスタに保存された測定値が変更されます。測定値の変更によって、暗号とハードウェアから導出された**システム測定値ルート鍵（SMRK）**が別の値へと変わり、その結果、鍵階層でシールの封印が壊れます。これにより**システム測定値デバイス鍵（SMDK）**がアクセス不能となり、その結果KEKが、そしてデータがアクセス不能となります。

ただし、システムが攻撃を受けていないときは、ファームウェアの測定値およびLocalPolicyの`nsih`フィールドが新規のmacOS測定値を指すように変更する正規のソフトウェアアップデートに対応する必要があります。信頼できると分かっている情報源を持たないようなほかのシステムがファームウェア測定値の取り込みを試みる場合、ユーザはセキュリティを無効にし、ファームウェアをアップデートしてから、再びセキュリティを有効にする必要があります。これは、新しい測定値ベースラインを取得するためです。これによって、ソフトウェアアップデート中に攻撃者がファームウェアを改ざんするリスクが大幅に高まります。Image4マニフェストが必要なすべての測定値を含んでいることがシステムの役に立っています。通常ブート中に測定値が一致したときにSMDKをSMRKと共に復号するハードウェアは、提示された将来のSMRKへとSMDKを暗号化することもできます。ソフトウェアアップデート後に予期される測定値を指定することで、ハードウェアは現在のオペレーティングシステムでアクセス可能なSMDKを暗号化し、将来のオペレーティングシステムでもアクセス可能とすることができます。同様に、お客様がLocalPolicyのセキュリティ設定を正規に変更したときは、LLBが次回の再起動で計算するLocalPolicyの測定値に基づいて、SMDKが将来のSMRKへと暗号化される必要があります。

Apple File Systemの役割

Apple File System（APFS）は、暗号化を念頭に設計されたApple独自のファイルシステムです。APFSは、Appleのすべてのプラットフォーム（iPhone、iPad、Mac、Apple TV、およびApple Watchのプラットフォーム）で機能します。フラッシュ/SSDストレージ向けに最適化され、強力な暗号化、コピーオンライトメタデータ、領域共有、ファイルとディレクトリのクローン作成、スナップショット、ディレクトリサイズの高速計算、アトミックセーフセーブプリミティブ、ファイルシステム基盤の改良が実現されたほか、I/Oとの統合による独自のコピーオンライト設計によってデータの信頼性を確保しながらパフォーマンスを最大限に引き出します。

スペース共有

APFSでは、ストレージ領域がオンデマンドで割り当てられます。1つのAPFSコンテナに複数のボリュームが含まれる場合は、コンテナの空き領域が共有され、必要に応じて個々のボリュームに割り当てられます。各ボリュームではコンテナ全体の一部のみが使用されるため、空き領域は、コンテナの合計サイズから、コンテナに含まれるすべてのボリュームの使用領域を差し引いたサイズになります。

複数ボリューム

macOS 10.15以降では、Macの起動に使用されるAPFSコンテナには少なくとも、次の5つのボリュームが必要です。最初の3つはユーザには表示されません:

- プリブートボリューム: このボリュームは暗号化されません。コンテナ内の各システムボリュームを起動するために必要なデータが格納されます。
- VMボリューム: このボリュームは暗号化されません。暗号化されたスワップファイルを保存するためにmacOSによって使用されます。
- リカバリボリューム: このボリュームは暗号化されません。recoveryOSで起動するために、システムボリュームをロック解除することなく利用できる必要があります。
- システムボリューム: 以下のものが格納されます。
    - Macを起動するために必要なすべてのファイル
    - macOSによってネイティブにインストールされるすべてのアプリ(以前「/アプリケーション」フォルダに置かれていたアプリは、現在「/システム/アプリケーション」に置かれています)

    注記: デフォルトでは、Appleのシステムプロセスを含め、いかなるプロセスもシステムボリュームには書き込みできません。
- **データボリューム:** 以下のような、変更されることのあるデータが格納されます。
    - ユーザのフォルダ内のデータ(写真、ミュージック、ビデオ、書類を含む)
    - ユーザがインストールしたアプリケーション(AppleScript、Automatorアプリケーションを含む)
    - ユーザ、組織、他社製アプリによってインストールされたカスタムのフレームワークとデーモン
    - ユーザが所有しているか書き込み可能なその他の場所(/アプリケーション、/ライブラリ、/ユーザ、/Volumes、/usr/local、/private、/var、/tmp)

追加される各システムボリュームにデータボリュームが作成されます。プリブートボリューム、VMボリューム、およびリカバリボリュームはすべて共有され、複製されません。

macOS 11以降では、システムボリュームがスナップショットでキャプチャされます。オペレーティングシステムは、ミュート可能なシステムボリュームの読み取り専用マウントからだけではなく、システムボリュームのスナップショットからもブートします。

iOSとiPadOSでは、ストレージが少なくとも2つのAPFSボリュームに分割されます。

- システムボリューム
- データボリューム

キーチェーンのデータ保護

多くのアプリ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。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。Appleのさまざまなオペレーティングシステムでは、種々のキーチェーン保護クラスと関連付けられた保証を適用するために、それぞれ異なるメカニズムが使用されています。macOS（Appleシリコン搭載Macを含む）では、これらの保証を適用するのにデータ保護が直接使用されることはありません。

概要

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キー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）は対応する秘密鍵で暗号化されます。メタデータキーはSecure Enclave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、各プロセスやアプリ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アプリの「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アプリ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アプリ間でのみ可能です。キーチェーン項目を共有するために、他社製アプリはアプリケーショングループのApple Developer Program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を使用します。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、固有の鍵と機能が使用されます。

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

バックグラウンド更新サービスを利用するアプリは、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。

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またはiPadOS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。

キーチェーンデータのクラス保護

以下のクラス保護がキーチェーン項目に適用されます。

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
Microsoft Exchange ActiveSync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鍵	初回ロック解除後
iCloudトークン	初回ロック解除後
iMessageキー	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
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
Finder/iTunesバックアップ	ロック解除時、移行不可
VPN証明書	初回ロック解除後、移行不可
Bluetooth®キー	常時、移行不可
Appleプッシュ通知サービス(APNs)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
SIM PIN	常時、移行不可
「探す」トークン	常時
留守番電話	常時

macOSでは、構成プロファイルによってインストールされたすべてのキーチェーン項目は**常時**利用可能です。iOSとiPadOSでは、構成プロファイルによってインストールされたキーチェーン項目は、種類、参照方法、インストールのタイミングによって、アクセスできるタイミングが異なります。デフォルトでは、構成プロファイルを使用してインストールされたキーチェーン項目は、**初回ロック解除後に利用可能となり、移行不可**です。ただし、構成プロファイルによってインストールされたキーチェーン項目でも、以下の場合には**常時**利用可能となります:

- iOS 15以降、iPadOS 15以降にアップグレードする前にインストールされた
- 証明書である(識別情報ではない)
- `com.apple.mdm`ペイロードの`IdentityCertificateUUID`によって参照された識別情報である

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。Face IDやTouch IDの使用またはデバイスのパスコードまたはパスワ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Face IDまたはTouch 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。

macOSのキーチェーンアーキテクチャ

さらにmacOSではキーチェーンにアクセスして、ユーザの名前とパスワード、デジタル署名、暗号鍵、秘密のメモなどを便利かつ安全に保存できます。キーチェーンにアクセスするには、「/アプリケーション/ユーティリティ/」にあるキーチェーンアクセスアプリケーションを使用します。キーチェーンを使用すれば、リソースごとに資格情報を入力する手間を省くことができ、覚えておく必要もなくなります。Macユーザごとに初期のデフォルトキーチェーンが1つ作成されます。また、目的に応じた追加のキーチェーンをユーザが作成することもできます。

macOSでは、ユーザのキーチェーンに加えて、ネットワーク資格情報やPKI(公開鍵基盤)識別情報など、ユーザ固有ではない認証情報を保存するための、システムレベルのキーチェーンが多数使用されます。その1つである「システムルート」キーチェーンには、オンラインバンキングや電子商取引などの一般的なタスクを円滑化するためのインターネットPKIルート認証局(CA)証明書が保存されます。このキーチェーンは変更できません。また、組織内のサイトやサービスで検証を円滑に行うために組織が用意したCA証明書を管理対象のMacコンピュータに導入することもできます。

FileVault

macOSでのFileVaultによるボリュームの暗号化

Macコンピュータでは、保存されたすべてのデータを保護するための内蔵暗号化機能、FileVaultを利用できます。FileVaultでは、AES-XTSデータ暗号化アルゴリズムを使用して、内蔵ストレージデバイスとリムーバブルストレージデバイス上のボリューム全体が保護されます。

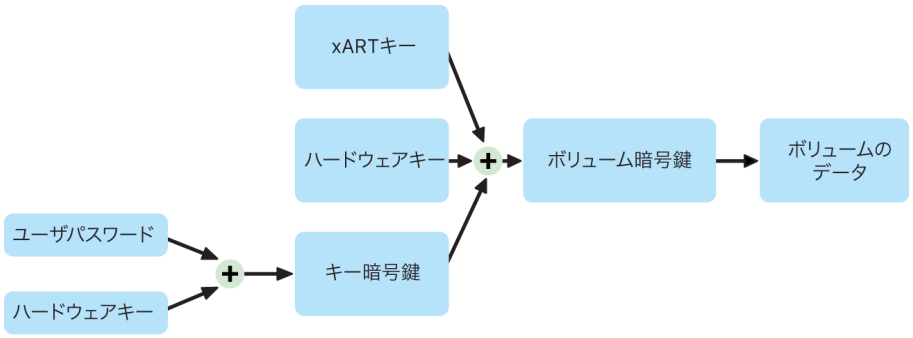
AppleシリコンMacのFileVaultは、データ保護クラスCをボリュームキーと共に使用して実装されています。AppleシリコンMacおよびApple T2セキュリティチップを搭載したMacの場合、Secure Enclaveに直接接続された内蔵ストレージデバイスの暗号化では、Secure EnclaveおよびAESエンジンのハードウェアセキュリティ機能が使用されます。ユーザがMacでFileVaultをオンにすると、ブートプロセス中にユーザの資格情報の入力を求められます。

注記: (1)**T2チップより前**のMacコンピュータ、(2)**最初からMacに搭載されていなかった**内部ストレージを搭載したMacコンピュータ、または(3)外部ストレージを接続したMacコンピュータ: FileVaultがオンになったあと、既存のすべてのファイルとさらに書き込まれたデータが暗号化されます。FileVaultをオンにする前に追加されてから削除されたデータは暗号化されず、フォレンジックデータ復旧ツールで復旧できる場合があります。

FileVaultがオンになっている内蔵ストレージ

有効なログイン資格情報や暗号化復旧キーがなければ、内蔵APFSボリュームは暗号化されたままで、物理ストレージデバイスを取り外して別のコンピュータに接続し直しても、不正アクセスからの保護が維持されます。macOS 10.15では、これにはシステムボリュームとデータボリュームの両方が含まれます。macOS 11以降、システムボリュームは署名済みシステムボリューム(SSV)機能によって保護されますが、データボリュームは引き続き暗号化によって保護されます。AppleシリコンまたはT2チップを搭載したMacでは、内蔵ボリュームの暗号化は、鍵の階層を構築して管理することで実装され、チップに内蔵されたハードウェア暗号化技術をベースにしています。この鍵の階層は、以下の4つの目的を同時に満たすように設計されています。

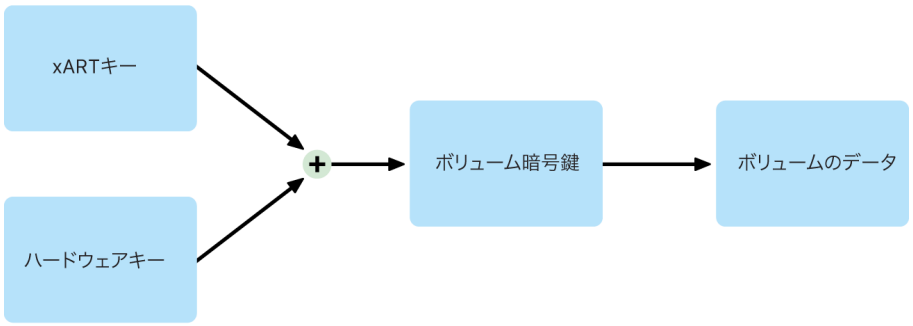
- 復号のためにユーザのパスワードを求める
- Macから取り外されたストレージメディアに対する直接的な総当たり(ブルートフォース)攻撃からシステムを守る
- 暗号化に必要な要素を削除することによってコンテンツを素早く安全にワイプするための方法を提供する
- ボリューム全体を暗号化し直さなくてもユーザがパスワードを変更できる(それに伴ってユーザのファイルを保護するための暗号鍵を変更できる)ようにする



AppleシリコンMacおよびT2チップを搭載したMacでは、FileVaultの鍵の処理はすべてSecure Enclave内で実行されます。そのため、暗号鍵がIntel CPUに直接公開されることはありません。デフォルトでは、APFSボリュームはすべて、ボリューム暗号鍵と共に作成されます。ボリュームとメタデータコンテンツはこのボリューム暗号化鍵で暗号化されます。この鍵は、鍵暗号化鍵(KEK)でラップされています。FileVaultがオンになっている場合、KEKはユーザのパスワードとハードウェアUIDの組み合わせで保護されます。

FileVaultがオフになっている内蔵ストレージ

AppleシリコンまたはT2チップを搭載したMacでは、初回のセットアップアシスタントのプロセス中にFileVaultをオンにしなかった場合でもボリュームが暗号化されます。ただし、ボリューム暗号鍵はSecure Enclave内のハードウェアUIDのみによって保護されます。



あとでFileVaultをオンにすると(データはすでに暗号化されているため処理はすぐに完了します)、アンチリプレイメカニズムによって、ハードウェアUIDのみに基づく古いキーがボリュームの復号に使用されなくなり、前述の通り、ユーザのパスワードとハードウェアUIDの組み合わせによってボリュームが保護されます。

FileVaultボリュームの削除

ボリュームを削除すると、そのボリューム暗号鍵がSecure Enclaveによって安全に削除されます。これにより、以後はSecure Enclaveでもこのキーにアクセスできなくなります。また、ボリューム暗号鍵はすべて、メディア鍵でラッピングされます。メディア鍵によってデータの機密性が高まるわけではありません。その代わりに、メディア鍵がないと復号は不可能であるため、メディア鍵を消去することでデータを素早く安全に削除できます。

AppleシリコンMacおよびT2チップを搭載したMacでは、Secure Enclaveが対応するリモートMDMコマンドなどのテクノロジーによって、メディア鍵が消去されることが保証されています。このようにしてメディア鍵を消去すると、ボリュームが暗号の仕組みによってアクセス不可になります。

リムーバブルストレージデバイス

リムーバブルストレージデバイスの暗号化では、Secure Enclaveのセキュリティ機能は使用されず、T2チップが搭載されていないIntelプロセッサ搭載Macと同じ方法で暗号化が行われます。

macOSでのFileVaultの管理

macOSでは、SecureTokenまたはブートストラップトークンを使用してFileVaultを管理できます。

セキュアトークンの使用

macOS 10.13以降のApple File System(APFS)では、FileVaultの暗号鍵の生成方法が変更されています。CoreStorageボリュームを使用する、以前のバージョンのmacOSでは、FileVaultの暗号化プロセスで使用する鍵は、ユーザまたは組織がMacでFileVaultをオンにした時点で作成されていました。APFSボリュームを使用するmacOSでは、ユーザの作成中、ユーザが初めてパスワードを設定するとき、またはユーザがMacに初めてログインするときに鍵が生成されます。この暗号鍵の実装、生成のタイミング、保存方法は、すべて**セキュアトークン**として知られている機能の一部です。セキュアトークンは、厳密には、ユーザのパスワードによって保護された、ラッピングされたキー暗号鍵(KEK)です。

APFSでFileVaultを使用する場合、以下のことが可能です。

- 既存のツールとプロセスを使用する(モバイルデバイス管理(MDM)ソリューションに保存できる個人の復旧キー(PRK)のエスクローなど)
- ユーザがMacにログインするかログアウトするまでFileVaultの有効化を保留する
- 組織の復旧キー(IRK)を作成して使用する

macOS 11では、Macで最初のユーザの初期パスワードを設定すると、そのユーザにセキュアトークンが付与されます。ワークフローによっては、これが望ましい動作ではなく、以前のように最初のセキュアトークンを付与するにはログインするためのユーザアカウントが必要な場合があります。このようなことが起きないようにするには、以下に示すように、ユーザのパスワードを設定する前に、プログラムで作成したユーザの`AuthenticationAuthority`属性に`;DisabledTags;SecureToken`を追加します。

```
sudo dscl . append /Users/<user name> AuthenticationAuthority
";DisabledTags;SecureToken"
```

ブートストラップトークンの使用

macOS 10.15では、モバイルアカウントと管理対象管理者(オプションでデバイス登録時に作成される管理者アカウント)の両方にセキュアトークンを付与するための新機能、**ブートストラップトークン**が導入されました。macOS 11では、ブートストラップトークンが、Macコンピュータにログインしているすべてのユーザ(ローカルユーザのアカウントを含む)にセキュアトークンを付与できます。macOS 10.15以降のブートストラップトークン機能を使用するには、以下の要件を満たす必要があります。

- Apple School ManagerまたはApple Business Managerを使用してMDMにMacを登録する(これによりMacを監視対象にする)
- MDMベンダーがこの機能をサポートしている

macOS 10.15.4以降では、Secure Tokenが有効になっているユーザが初めてログインしたときに、ブートストラップトークンが生成され、MDMにエスクローされます(MDMソリューションでこの機能がサポートされている場合)。必要に応じて、`profiles`コマンドラインツールを使用してブートストラップトークンを生成し、MDMにエスクローすることもできます。

macOS 11では、ブートストラップトークンがユーザアカウントへのセキュアトークンの付与以外にも使用される場合があります。Appleシリコン搭載Macでは、使用可能な場合はブートストラップトークンを使用して、MDMによる管理中にカーネル拡張機能とソフトウェアアップデートの両方のインストールを認証することができます。

組織の復旧キーと個人の復旧キー

CoreStorageボリュームおよびAPFSボリューム上のFileVaultは、どちらも組織の復旧キー(IRK。以前は**FileVaultマスターアイデンティティ**と呼ばれていました)によるボリュームのロック解除に対応しています。IRKはボリュームのロックを解除するかFileVaultを完全にオフにするコマンドライン操作のために便利ですが、特に最近のバージョンのmacOSでは、組織にとっての有用性は限られます。また、Appleシリコンを搭載したMacでは、IRKは主に2つの理由で機能的な価値を提供しません: まず、IRKを使用してrecoveryOSにアクセスすることはできません。次に、ターゲットディスクモードに対応しなくなったため、ボリュームを別のMacに接続してロックを解除することはできません。これらやその他の理由により、**Macコンピュータ上のFileVaultを組織で管理する場合にIRKを使用することは推奨されなくなりました。**代わりに、個人の復旧キー(PRK)を使用してください。

Appleがユーザの個人データを保護する方法

アプリのユーザデータへのアクセスの保護

保存されているデータが暗号化されるだけでなく、Appleデバイスでは、Data Vaultなどのさまざまなテクノロジーを使って、アプリ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。iOSおよびiPadOSの「設定」、およびmacOSの「システム設定」(macOS 13以降)または「システム環境設定」(macOS 12以前)で、ユーザは所定の情報へのアクセスをこれまでに許可しているアプリを確認できます。その後のアクセスを認めたり、アクセス権を取り消すことも可能です。以下の場合はアクセスが強制されます:

- **iOS、iPadOS、およびmacOS:** カレンダー、カメラ、連絡先、マイク、写真、リマインダー、および音声認識
- **iOSおよびiPadOS:** Bluetooth、ホーム、メディア、メディアアプリとApple Music、モーションとフィットネス
- **iOSおよびwatchOS:** ヘルスケア
- **macOS:** 入力監視(キーボードストロークなど)、プロンプト、画面収録(静止スクリーンショットやビデオなど)、および「システム設定」(macOS 13以降)またはシステム環境設定(macOS 12以前)

iOS 13.4以降およびiPadOS 13.4以降では、すべての他社製アプリのデータは自動的にData Vaultで保護されます。Data Vaultにより、サンドボックス化されていないプロセスのデータも不正アクセスから保護されます。iOS 15以降の追加クラスには、ローカルネットワーク、近くの機器との連携、リサーチセンサーおよび使用状況データ、集中モードがあります。

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は iOSおよびiPadOSのアプリに与えられます。「設定」の「iCloud」からそれぞれのアプリのアクセスを制御できます。また、iOSおよびiPadOSでは、モバイルデバイス管理(MDM)ソリューションによってインストールされたアプリおよびアカウントと、ユーザがインストールしたアプリおよびアカウントとの間で、データ移動を禁止するための制限を設定することもできます。

ユーザのヘルスケアデータへのアクセスの保護

HealthKitはiPhoneとApple Watch上のヘルスケアとフィットネスのデータのための中心的なレポジトリを提供します。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。HealthKitと、ヘルスケアおよびフィットネスアプリ、医療機関、ヘルスケアやフィットネス関連のデバイスとのやりとりには、すべてユーザの許可が必要です。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、Face IDまたはTouch 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。

ヘルスケアとフィットネスのデータを収集する/保存する

HealthKitでは、アプリに対するのアクセス権、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アプリを起動するスケジュール情報などの管理データも収集および保存できます。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、マージされたあとに削除されます。

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エンドツーエンドで暗号化するには、iOS 12以降と2ファクタ認証を使用する必要があります。この要件を満たさない場合でも、保管時と転送時にはユーザのデータが暗号化されますが、エンドツーエンドの暗号化ではありません。ユーザが2ファクタ認証を有効にして、iOS 12以降にアップデートすると、ユーザのヘルスケアデータがエンドツーエンドの暗号化に移行されます。

ユーザがFinder(macOS 10.15以降)またはiTunes(macOS 10.14以前)を使ってバックアップすると、バックアップが暗号化される場合にのみヘルスケアデータが保存されます。

診療記録

ユーザは、ヘルスケアアプリ内から対応するヘルスケアシステムにサインインして、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 1.3で保護された接続を使用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。

ヘルスケアデータの真正性

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所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アプリを特定するアプリ識別情報が含まれます。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のデータ真正性を確保するためです。デジタル署名には、RFC 5652で定められているCMS（Cryptographic Message Syntax）が使用されます。

ヘルスケアデータへの他社製アプリによるアクセス

HealthKit APIへのアクセスはエンタイトルメントで制御され、アプリは、データの利用方法に関する制限に従う必要があります。例えば、ヘルスケアデータを広告に使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。

アプリ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。アプリ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、「設定」>「ヘルスケア」>「データアクセスとデバイス」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。

アプリ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。アプリに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、アプリから、ほかのアプリ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、アプリ側でそのアプリ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。アプリ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です。これは、アプリが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をできなくするためです。

ユーザのメディカルID

ヘルスケアアプリでは、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アップデートを行います。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。iOS 13以前では、データはiCloudバックアップにバックアップされます。iOS 14では、メディカルIDはCloudKitを使用してデバイス間で同期され、その他のヘルスケアデータと同じ暗号化特性を持ちます。

ヘルスケア共有

iOS 15では、ユーザがヘルスケアアプリでほかのユーザとヘルスケアデータを共有するオプションがあります。ヘルスケアデータは2人のユーザ間でエンドツーエンドのiCloud暗号化を使用して共有され、ヘルスケア共有で送信されるデータにAppleがアクセスすることはできません。この機能を使用するには、送信側と受信側の両方のユーザがiOS 15以降を実行していて、2ファクタ認証を有効にしている必要があります。

ユーザはさらに、ヘルスケアアプリの「医療機関との共有」機能を使って、ヘルスケアデータを医療機関と共有することを選択することもできます。この機能を使用して共有されるデータは、ユーザが選択した医療機関のみがエンドツーエンドの暗号化を通して使用できます。Appleが暗号鍵を保持またはアクセスして、「医療機関との共有」機能で共有されたヘルスケアデータを復号、確認、その他の方法でアクセスすることはありません。このサービスの設計により、ユーザのヘルスケアデータがどのように保護されるのかについてさらに詳しくは、「医療機関向けApple登録ガイド」の「セキュリティとプライバシー」セクションを参照してください。

デジタル署名と暗号化

アクセス制御リスト

キーチェーンデータは、アクセス制御リスト(ACL)によって分離されて保護されます。このため、他社製アプリが保存した資格情報は、ユーザが明示的に許可しない限り、異なる識別情報を持つアプリからはアクセスできません。この保護機能により、組織内のさまざまなアプリおよびサービスに、Appleデバイス内の認証資格情報を保護するためのメカニズムが提供されます。

メール

「メール」アプリでは、デジタル署名して暗号化したメッセージを送信できます。「メール」によって、互換性のあるスマートカードに添付されたPIV(個人識別情報検証)トークン内のデジタル署名と暗号化証明書から、RFC 5322形式の大文字/小文字が区別される適切なメールアドレスのサブジェクトまたはサブジェクト代替名が自動的に検出されます。設定されたメールアカウントが、添付されたPIVトークン内のデジタル署名または暗号化証明書に含まれるメールアドレスと一致すると、新規メッセージウインドウのツールバーに、署名ボタンが自動的に表示されます。送信先のメール暗号化証明書が「メール」内にある場合、またはMicrosoft Exchangeのグローバルアドレス一覧(GAL)で見つかった場合は、新規メッセージのツールバーに、開いたカギのアイコンが表示されます。閉じたカギのアイコンは、送信先の公開鍵によってメッセージが暗号化されて送信されることを示します。

メッセージごとのS/MIME

iOS、iPadOS、macOSでは、メッセージごとのS/MIMEがサポートされます。これにより、S/MIMEユーザは、メッセージの署名と暗号化をデフォルトで常に行うか、メッセージごとに判断するかを選択できます。

S/MIMEで使用する識別情報は、構成プロファイル、モバイルデバイス管理(MDM)ソリューション、Simple Certificate Enrollment Protocol(SCEP)、またはMicrosoft Active Directory認証局を使用してAppleデバイスに配付できます。

スマートカード

macOS 10.12以降では、PIVカードがネイティブでサポートされます。PIVカードは、企業や政府機関で、2ファクタ認証、デジタル署名、暗号化のために幅広く使用されています。

スマートカードには、公開鍵と秘密鍵のペアおよび関連する証明書が含まれる、1つ以上のデジタル識別情報が組み込まれます。PIN（個人識別番号）でスマートカードをロック解除すると、認証、暗号化、署名の操作に使用する秘密鍵にアクセスできます。証明書では、鍵の用途、関連付けられた属性、認証局（CA）認証によって検証（署名）済みかどうかが判断されます。

スマートカードは2ファクタ認証にも使用できます。カードをロック解除するには、「ユーザが持っているもの」（カード自体）と「ユーザが知っていること」（PIN）の2つの要素が必要です。macOS 10.12以降では、スマートカードによるログインウインドウ認証とSafariでのWebサイトへのクライアント証明書認証もネイティブで対応します。また、Kerberos対応サービスにシングルサインオンするための、鍵ペアを使用したKerberos認証（PKINIT）もサポートされます。スマートカードとmacOSについて詳しくは、「**Appleプラットフォーム導入**」の「スマートカードの統合の概要」を参照してください。

暗号化ディスクイメージ

macOSでは、暗号化ディスクイメージは、ユーザが機密書類やその他のファイルを安全に保管または受け渡しするためのコンテナとして使用できます。暗号化ディスクイメージは、「/アプリケーション/ユーティリティ/」にあるディスクユーティリティを使用して作成します。ディスクイメージの暗号化には、128ビットまたは256ビットのAES暗号化が使用されます。マウントされたディスクイメージは、Macに接続されたローカルボリュームとして扱われるため、ユーザは、イメージ内に保存されたファイルやフォルダをコピーしたり、移動したり、開いたりできます。FileVaultと同様に、ディスクイメージのコンテンツは、リアルタイムで暗号化および復号されます。ユーザは、暗号化ディスクイメージをリムーバブルメディアに保存したり、メールメッセージに添付して送信したり、リモートサーバに保存したりすることで、書類、ファイル、フォルダを安全にやりとりできます。暗号化ディスクイメージについて詳しくは、「ディスクユーティリティユーザガイド」を参照してください。

アプリのセキュリティ

アプリのセキュリティの概要

現在、アプリは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。アプリは生産性においてすばらしいメリットをもたらすと同時に、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、Appleでは複数の保護レイヤーを構築し、アプリが既知のマルウェアに感染していないこと、および改ざんされていないことを保証しています。アプリからユーザデータへのアクセスを注意深く仲介するための追加の保護も適用されます。これらのセキュリティ制御によって安定した安全なアプリ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iOS、iPadOS、およびmacOS用の数十万ものアプリを、システムの整合性を損なうことなく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、Appleデバイス上のこれらのアプリに安心してアクセスできるようになります。

最も厳重な制御を行うため、iPhoneとiPadでは、すべてのアプリはApp Storeから取得され、かつサンドボックス化されます。

Macでは、多くのアプリがApp Storeから取得されますが、Macユーザはインターネットからもアプリをダウンロードして使用します。インターネットからのダウンロードを安全にサポートするため、macOSには制御層がさらに追加されています。まず、macOS 10.15以降、Appleからの公証を受けていないMacアプリはデフォルトで起動できなくなります。この要件により、App Storeで提供されているアプリでなくても、それらのアプリが既知のマルウェアに感染していないことが保証されます。さらに、macOSには、マルウェアをブロックし、必要に応じて削除するための最先端のアンチウイルス保護が含まれています。

アプリによる不正アクセスからユーザデータを保護するのに有効なサンドボックス化が、プラットフォーム全体にわたるさらなる制御をもたらします。さらにmacOSでは、重要な領域内のデータ自体が保護されます。その結果、アクセスしようとしているアプリがサンドボックス化されているかどうかにかかわりなく、デスクトップ、書類、ダウンロード、その他の領域にあるファイルへのすべてのアプリからのアクセスをユーザが確実に制御し続けることができます。

ネイティブの機能	他社製の同等機能
プラグイン未承認リスト、Safari機能拡張未承認リスト	ウイルス/マルウェア定義
ファイルの隔離	ウイルス/マルウェア定義
XProtect/YARAシグネチャ	ウイルス/マルウェア定義。エンドポイント保護
Gatekeeper	エンドポイント保護: アプリのコード署名を徹底させることで、信頼されたソフトウェアのみが動作することを保証
eficheck (Apple T2セキュリティチップを搭載していないMacの場合は必須)	エンドポイント保護。ルートキットの検出
アプリケーションファイアウォール	エンドポイント保護。ファイアウォール機能

ネイティブの機能	他社製の同等機能
パケットフィルタ(PF)	ファイアウォールソリューション
システム整合性保護	macOS内蔵
強制アクセス制御	macOS内蔵
kext除外リスト	macOS内蔵
必須のアプリコード署名	macOS内蔵
アプリの公証	macOS内蔵

iOSおよびiPadOSでのアプリのセキュリティ

iOSおよびiPadOSでのアプリのセキュリティの概要

ほかのモバイルプラットフォームとは異なり、iOSおよびiPadOSでは、ユーザは悪意のある可能性のある未署名のアプリをWebサイトからインストールしたり、信頼されていないアプリを実行したりすることはできません。そのため、(EU以外では)すべてのアプリはApp Storeからダウンロードする必要があります。App Storeでは、すべてのアプリが特定できるデベロッパから提供されており、自動および人間による審査を通過しなければなりません。実行時には、ページが読み込まれるときに、すべての実行可能ファイルのメモリページの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アプリが改変されていないことを確認できます。

アプリ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、ほかのアプリやシステムのほかの部分が侵害されるのを防止するためのiOSおよびiPadOSのセキュリティ対策が強制的に適用されます。

App Storeのセキュリティについて

App Storeは、ユーザが安全にアプリを見つけてダウンロードできる、信頼できる場所です。App Storeのアプリは、Appleのガイドラインに従うことに同意した特定できるデベロッパから提供され、ユーザに安全に配布されて、改変されていないことが暗号によって保証されます。すべてのアプリと、すべてのアプリのアップデートは、プライバシー、セキュリティ、安全性の要件を満たしているかどうかを評価するために、審査されます。このプロセスは、マルウェア、サイバー犯罪、詐欺をApp Storeから排除し続けることによってユーザを守れるように設計されており、常に改善を続けています。さらに、お子様向けのアプリは、お子様の安全を守るために策定されたデータ収集とセキュリティに関する厳格なガイドラインに従い、iOSおよびiPadOSのペアレンタルコントロール機能と緊密に統合する必要があります。

App Storeのセキュリティ保護には、以下の内容が含まれます:

- **既知のマルウェアの自動スキャン:** App Storeに紛れ込み、ユーザのデバイスに侵入したり、被害を与えたりすることがないようにします。
- **人間のエキスパートチームによる審査:** 正確を期すため、マーケティングのテキストやスクリーンショットを含むアプリの説明を審査します。これは、マルウェアを人気アプリと偽る、実際には搭載されていない魅力的な機能を提供すると主張するなど、マルウェアの配布に特によく使われる詐欺に対して高い障壁になります。
- **手動チェック:** アプリが不必要に機密データへのアクセスをリクエストしないことを確認します。また、厳格なデータ収集および安全ルールに確実に準拠できるように、お子様向けのアプリに対して追加の評価を実施します。
- **信頼性の高い一元的なユーザレビュー:** 問題を明らかにすることで、攻撃者が多くのユーザを欺く可能性を大幅に減らします。悪意のあるアプリが審査プロセスでその動作を完全に隠すことができたとしても、アプリのユーザが問題に遭遇して報告することで、ほかのユーザやAppleに警告することができるので、別の検出手段を提供することになります。このシグナルの価値を高めるため、App Storeは積極的に不正レビュー対策を行っています。

- **修正と削除のプロセス:** 問題が発生した場合に備えます。アプリがApp Storeに登録され、のちにガイドライン違反が発覚した場合、Appleはデベロッパと協力して迅速な問題解決に当たります。詐欺や悪意のある行為に関連する危険なケースでは、アプリは即座にApp Storeから削除されます。そのアプリをダウンロードしたユーザには、アプリの悪質な行為についての通知を送ることができます。

iOSおよびiPadOSでのアプリのセキュリティは、すべてのレイヤーの組み合わせ、すなわち悪意のあるアプリのインストールを防ぐための厳格なアプリの審査と、悪意のあるアプリによる被害を制限する厳格なプラットフォーム保護によります。iOSおよびiPadOSのセキュリティ設計は、あらゆるコンシューマデバイスの中で最も強力な保護を提供しますが、ユーザがだまされて行う可能性のある行為に対する保護を提供することはできません。アプリの審査によって、App Storeポリシーへの準拠が保証されます。App Storeポリシーは、ユーザに被害を与えようとするアプリや、ユーザをだまして機密データへのアクセスを付与させようとするアプリからの保護を目的として策定されています。また、悪意のあるアプリがデバイスの保護を迂回するという非常に深刻な事例でも、アプリの審査によって、そもそもそういったアプリがユーザのデバイスに侵入するのが難しくなります。

App Storeのセキュリティ対策だけで万全を期すことはできませんが、これはプラットフォームのセキュリティを保つための徹底した防衛戦略の一環であり、そのおかげで、金銭目的の攻撃者がiOSやiPadOSユーザに対して広範な攻撃を行うことは現実的、経済的でないものになっています。すべてのアプリをApp Storeで公開される前に審査することで、マルウェアを排除し、正確な情報をユーザに伝えることができます。また、アプリが有害であることが判明した場合は、すぐにアプリの配布をやめることで、今後の亜種の拡散を制限することができます。こういった対策により、Appleはエコシステムのセキュリティを保護し、お客様に安心を与えています。

iOSおよびiPadOSのアプリコード署名プロセス

iOSおよびiPadOSでは、必須のコード署名、厳密なデベロッパによるサインインなどによってアプリのセキュリティが提供されています。

必須のコード署名

iOSまたはiPadOSのカーネルが起動すると、どのユーザプロセスとアプリの実行を許可するかをカーネルが制御します。すべてのアプリ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およびiPadOS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アプリは、Appleによって署名されています。他社製アプリも、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必須とすることで、信頼チェーンの概念をオペレーティングシステムのみならずアプリにまで適用することができ、他社製アプリ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。

デベロッパがアプリに署名する方法

デベロッパは（Apple Developer Programを通じた）証明書の検証を通じてアプリに署名することができます。フレームワークをアプリに埋め込み、そのコードを（チーム識別文字列を通じて）Appleが発行した証明書で検証することができます。

- **証明書の検証:** アプリを開発してiPhoneまたはiPad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あとに証明書が発行されます。この証明書によって、デベロッパはアプリに署名し、アプリを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にあるすべてのアプリは、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、これは悪意のあるアプリ開発に対する抑止力にもなります。また、Appleは、アプリが通常説明の通りに動作し、明らかなバグや何らかの目立つ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、ユーザはアプリ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。

- **コード署名の検証:** iOSおよびiPadOSでは、デベロッパがアプリ内にフレームワークを埋め込み、そのフレームワークをアプリ自体またはアプリ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アプリ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情報(チームID)を使って実施されます。チーム識別情報は、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情報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付属する実行可能ファイルにはチーム識別情報がないため、システム自体に付属するライブラリにのみリンクできます。

独自の社内アプリの検証

適格な企業は組織内で使用するための独自の社内アプリを開発して、従業員に配付することができます。企業や組織はApple Developer Enterprise Program(ADEP)に申請できます。詳しい情報や資格の要件を確認するには、Apple Developer Enterprise ProgramのWebサイトを参照してください。組織がADEPに登録されると、承認したデバイスで独自の社内アプリ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。

ユーザがこれらのアプリを実行するには、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、組織のアプリをiPhoneやiPadに読み込めません。モバイルデバイス管理(MDM)でインストールされたアプリは、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。それ以外のアプリについては、ユーザが「設定」でアプリ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アプリをユーザが承認しないように制限することもできます。どの独自の社内アプリでも、初回起動時に、アプリ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。

iOSおよびiPadOSでのランタイムプロセスのセキュリティ

iOSおよびiPadOSでは、「サンドボックス」、エンタイトルメントの宣言、およびアドレス空間配置のランダム化(ASLR)の使用によってランタイムのセキュリティを確保します。

サンドボックス化

他社製アプリはすべて「サンドボックス化」されるので、ほかのアプリ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。サンドボックス化は、ほかのアプリ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ために行われます。各アプリ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、これはアプリ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。他社製アプリ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およびiPadOS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アプリから保護されます。iOSとiPadOSのほとんどのシステムファイルとリソースは、他社製アプリと同様に特権のないユーザ「mobile」として実行されます。オペレーティングシステム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、アプリがAPIを使って自身の権限を昇格させてほかのアプリやiOSおよびiPadOSを変更することもできません。

エンタイトルメントの使用

他社製アプリによるユーザ情報やiCloudや拡張機能などの機能へのアクセスは、エンタイトルメントの宣言により制御されます。エンタイトルメントは、アプリに含まれる署名されたキー値とのペアで、UNIXユーザIDのようなランタイム要素を越えた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、システムアプリやデーモンが特権を必要とする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、不正なシステムアプリ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、アプリ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、アプリ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

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。内蔵アプリは、ASLRを使用して、起動時にすべてのメモリ領域を確実にランダム化できます。起動時の動作に加えて、ASLRによって実行コード、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がさらに低減します。例えば、「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をランダムに配置することにより、その攻撃の実行がより困難になります。複数のデバイスを標的とする場合は特にそうです。iOSおよびiPadOS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。

Execute Never機能

iOSおよびiPadOS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、厳しく管理された条件を満たすアプリ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は、JavaScriptジャストインタイム（JIT）コンパイラでこの機能を使用しています。

iOS、iPadOS、およびmacOSでの機能拡張のサポート

iOS、iPadOS、およびmacOSでは、機能拡張を提供することで、アプリの機能をほかのアプリに提供できます。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、アプリ内にパッケージ化されています。アプリ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アプリで利用できるようになります。

拡張ポイント

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アプリに制限できます。例えば、「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。拡張ポイントの例としては、「今日」ウィジェット、共有、アクション、写真編集、ファイルプロバイダ、カスタムキーボードなどがあります。

機能拡張との通信方法

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アプリ間の通信には、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、機能拡張を含むアプリ本体、および機能拡張を使用するアプリからは互いに分離されるように設計されています。ほかの他社製アプリと同様にサンドボックス化され、機能拡張を含むアプリ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、アプリ本体と同じものになります。そのため、ユーザがアプリに「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アプリに埋め込まれた機能拡張に対しては適用されますが、そのアプリが起動する別のアプリの機能拡張には適用されません。

カスタムキーボードの使用方法

カスタムキーボードは特殊な種類の機能拡張であり、ユーザがシステム全体に対して有効にするものです。キーボード機能拡張が有効になると、パスコード入力とセキュリティ保護されたテキストの表示を除くすべてのテキストフィールドで使用されます。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えいが可能な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あと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と機能拡張

モバイルデバイス管理(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。例えば、MDMソリューションは、ユーザが管理対象アプリ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、管理対象アプリ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、アプリのデベロッパはアプリ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。

iOSおよびiPadOSでのアプリ保護とアプリグループ

iOSおよびiPadOSでは、iOS SDKの使用によって、およびApple Developer Portalでアプリグループに参加することで、アプリを安全に保護できます。

アプリでのデータ保護の採用

iOSおよびiPadOSのSoftware Development Kit(SDK)には、社内外のデベロッパが簡単にデータ保護を採用し、最高レベルの保護をアプリ内で達成できるようにするための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。

メールアプリのデータベース(添付ファイルを含む)、管理対象のブック、Safariブックマーク、アプリの起動イメージ、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`Data Protection`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アプリのうち、特定のデータ保護クラスに所属していないアプリには、デフォルトでProtected Until First User Authenticationが割り当てられます。

アプリグループへの参加

特定のデベロッパアカウントが所有するアプリと機能拡張では、アプリ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、目的のアプリと機能拡張をそのグループに追加できます。アプリグループのメンバーとして構成されると、アプリ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(そのグループのアプリが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、アプリのエコシステム全体でのアプリグループID(GID)の一意性が確保されます。

macOSアプリのセキュリティ

macOSでのアプリのセキュリティの概要

macOSのアプリのセキュリティは、いくつかの重複する層で構成されます。最初の層は、App Storeで提供される署名され信頼されたアプリのみを実行するオプションです。また、macOSの保護レイヤーにより、インターネットからダウンロードしたアプリが既知のマルウェアに感染していないことが保証されます。macOSは、マルウェアを検出して削除するテクノロジーを備えており、信頼されていないアプリからのユーザデータへのアクセスを防ぐ追加の保護機能も搭載しています。公証やXProtectのアップデートなどのAppleのサービスは、マルウェアのインストールを防止するように設計されています。必要時には、これらのサービスが最初の検出を逃れた可能性のあるマルウェアを見つけ、素早く効率的に削除します。最後に、利便性を損なわないようにセキュリティモデル内でアプリを操作できる仕組みがあります。これで、まったくの未署名で信頼されていないコードを実行する場合にも対応できます。

macOSでのアプリのコード署名プロセス

App Storeから取得したすべてのアプリには、Appleの署名が付いています。この署名は、改ざんや変更がなされていないことを保証するためのものです。Appleデバイスに付属するアプリにはAppleが署名しています。

App Store外で配付されるアプリについては、macOS 10.15以降、デベロッパがApple発行の（秘密鍵が設定された）デベロッパID証明書を使って署名し、Appleから公証を受けない限り、デフォルトのGatekeeper設定下では実行できません。社内開発のアプリも、ユーザが整合性を検証できるようにApple発行のデベロッパIDで署名してください。

macOSではコード署名と公証プロセスは互いに独立しており、同じ人が実施する必要はありません。これは目的が異なるからです。コード署名は、デベロッパにより、（Apple発行の）デベロッパID証明書を使用して行われます。この署名の検証によって、デベロッパがソフトウェアを開発および署名して以降、そのソフトウェアが改ざんされていないことがユーザに証明されます。公証はソフトウェア配付チェーン内のだれでも実施できます。これには、Appleがマルウェアのチェックのためにコードのコピーの提出を受け、既知のマルウェアが検出されなかったことを保証する目的があります。公証結果はチケットとしてAppleのサーバに保管され、必要に応じて（だれでも）アプリに付加できます。付加によってデベロッパの署名が無効になることはありません。

強制アクセス制御（MAC）では、システムによって保護されるエンタイトルメントを有効にするためにコード署名が要求されます。例えば、ファイアウォール経由のアクセスを要求するアプリには、適切なMACエンタイトルメントを伴うコード署名が必要です。

macOSでのGatekeeperおよびランタイム保護

macOSには、信頼されたソフトウェアのみがユーザのMac上で動作することを保証するGatekeeperテクノロジーおよびランタイム保護機能が搭載されています。

Gatekeeper

macOSには、信頼されたソフトウェアのみがユーザのMac上で動作することを保証するように設計された、**Gatekeeper**と呼ばれるセキュリティテクノロジーが搭載されています。ユーザがApp Storeの外からアプリ、プラグイン、またはインストーラパッケージをダウンロードして開くと、Gatekeeperは、そのソフトウェアの提供元がIDを有するデベロッパであり、そのソフトウェアに既知の悪質なコンテンツがないとAppleが公証し、ソフトウェアが改変されていないことを確認します。Gatekeeperはさらに、ダウンロードしたソフトウェアを初めて開く際にユーザの承認を求めます。単なるデータファイルだとユーザに信じ込ませて何らかの実行コードを実行する策略ではないと確認するためです。また、Gatekeeperは、ダウンロードしたソフトウェアによって書き込まれたファイルの出所も追跡します。

デフォルトでは、Gatekeeperによって、ダウンロード済みのすべてのソフトウェアが、App Storeで署名されている、または登録済みのデベロッパが署名し、かつAppleで公証されていることが保証されます。App Storeのレビュープロセスと公証パイプラインはどちらも、アプリに既知のマルウェアが含まれていないことを保証するように設計されています。そのためデフォルトでは、**macOSのすべてのソフトウェアは、どのような経路でMacに入ったかに関係なく、既知の悪意あるコンテンツが含まれていないかが最初に開かれるときにチェックされます**。

ユーザや組織は、App Storeからインストールされたソフトウェアのみを許可するように設定できます。またはユーザは、モバイルデバイス管理（MDM）ソリューションで制限されていない限りどのソフトウェアでも開くように、Gatekeeperのポリシーを無効にできます。組織は、代替のIDによるソフトウェアの署名を許可するなど、MDMを使用してGatekeeperの設定を変更できます。状況に応じてGatekeeperを完全に無効にすることもできます。

Gatekeeperは、無害なアプリを経由した悪質なプラグインの配付からも保護します。このようなアプリを使用すると、ユーザが知らないうちに悪質なプラグインが読み込まれてしまいます。Gatekeeperは必要に応じて、ランダム化された読み出し専用の場所からアプリを開きます。これは、アプリと共に配付されるプラグインの自動読み込みを防ぐための動作です。

ランタイム保護

システムファイル、リソース、およびカーネルは、ユーザのアプリ空間から保護されています。App Storeから取得したアプリはすべてサンドボックス化されており、ほかのアプリによって保存されたデータへのアクセスが制限されています。App Storeから取得したアプリで別のアプリのデータにアクセスする必要がある場合は、必ずmacOSで提供されているAPIおよびサービスを使用する必要があります。

macOSでのマルウェアからの保護

Appleはマルウェアを素早く検出してブロックするための脅威インテリジェンスプロセスを運用しています。

3つの防御層

マルウェアからの防御は以下の3つの層で構成されています:

1.**マルウェアの起動と実行の防止:** App Store、または公証と組み合わせたGatekeeper

2.**お客様のシステムでのマルウェア実行をブロック:** Gatekeeper、公証、およびXProtect

3.**実行されたマルウェアへの対処:** XProtect

初めの防御層は、マルウェアの配付を阻止し、1回たりとも起動させないように設計されています。これはApp Storeや、公証と組み合わせたGatekeeperの目指すことです。

次の防御層は、Mac上に出現したマルウェアを素早く検出およびブロックすることで、マルウェアの拡散を防ぐだけでなく、すでにマルウェアが足場を築いてしまったMacシステムを修復できるようにします。この防御は、XProtect、さらにGatekeeperと公証によって強化されます。

最後にXProtectが動作し、実行に成功したマルウェアに対処します。

これらの保護（以下で詳しく説明します）を組み合わせて、ウイルスやマルウェアからの最も効率的な保護の実現をサポートします。ほかにも保護は存在し、特にAppleシリコン搭載Macには、実行に成功したマルウェアが引き起こすおそれのある損害を制限するための保護があります。macOSがユーザデータをマルウェアから保護する方法についてはアプリのユーザデータへのアクセスの保護を、macOSがマルウェアのシステム上での動作を制限する方法についてはオペレーティングシステム整合性を参照してください。

公証

公証とは、Appleが提供するマルウェアスキャンサービスです。App Store外でmacOS用のアプリを配付したいデベロッパは、配付プロセスの一環として、アプリを提出してスキャンを受けます。Appleはそのアプリをスキャンし、既知のマルウェアが見つからなければ公証チケットを発行します。デベロッパは通常このチケットをアプリに付加し、Gatekeeperがそのアプリをオフラインでも検証および起動できるようにします。

また、たとえ以前に公証されていても、悪意があると分かっているアプリには、Appleが取り消しチケットを発行することがあります。macOSは定期的に新しい取り消しチケットをチェックすることで、Gatekeeperが最新情報を得て、そのようなファイルの起動をブロックできるようにします。このプロセスによって、悪意のあるアプリを非常に素早くブロックできます。これは、バックグラウンドで行われる取り消しチケットのアップデートが、新しいXProtectシグネチャをプッシュするバックグラウンドアップデートよりもはるかに頻繁に行われるためです。さらにこの保護は、以前に公証を受けたアプリと、まだ公証を受けていないアプリの両方に適用できます。

XProtect

macOSには**XProtect**と呼ばれるアンチウイルステクノロジーが組み込まれており、署名に基づいたマルウェアの検出と削除が可能です。このシステムは、署名を基にマルウェアを検出するYARAシグネチャというツールを使用します。このツールはAppleによって定期的にアップデートされます。Appleは新しいマルウェアの感染と傾向を監視しており、Macをマルウェアの感染から効果的に防御するため、システムアップデートとは別にシグネチャを自動的にアップデートしています。XProtectによって既知のマルウェアが自動的に検出され、その実行がブロックされます。macOS 10.15以降では、以下のタイミングでXProtectによる既知の悪質なコンテンツのチェックが実行されます:

- アプリが初めて起動されたとき
- アプリが変更されたとき（ファイルシステム内で）
- XProtectシグネチャがアップデートされたとき

XProtectで既知のマルウェアが検出されると、そのマルウェアがブロックされ、ユーザに通知されます。ユーザはマルウェアをゴミ箱に移動できます。

注記: 公証は、既知のファイル（またはファイルハッシュ）に対して有効であり、以前に起動されたことのあるアプリで使用できます。XProtectのシグネチャに基づいたルールは具体的なファイルハッシュよりも汎用性が高いため、Appleが未確認の変種も発見できます。XProtectがスキャンを行うのは、アプリが変更されたときと初めて起動されたときのみです。

万一マルウェアがMacに侵入している場合でも、XProtectには感染に対処するためのテクノロジーがあります。例えば、（システムデータファイルやセキュリティアップデートの自動アップデートの一環として）Appleから自動的に配信されるアップデートに基づいて感染に対処するエンジンが含まれます。このシステムは、アップデートされた情報を受け取るとマルウェアを削除し、引き続き定期的に感染しているかどうかを確認します。ただし、XProtectにはMacを自動的に再起動する機能はありません。さらに、XProtectには行動分析に基づいて未知のマルウェアを検出するための高度なエンジンが含まれています。このエンジンによって検出されるマルウェアに関する情報は、最終的にそのマルウェアのダウンロードを行ったソフトウェアを含め、XProtectシグネチャとmacOSのセキュリティの向上に使用されます。

自動XProtectセキュリティアップデート

Appleは、利用可能な最新の脅威インテリジェンスに基づいたXProtectのアップデートを自動的に発行します。デフォルトでは、macOSはこれらのアップデートを毎日チェックします。公証のアップデートはCloudKit同期によって配付され、XProtectのアップデートよりもはるかに頻繁に行われます。

新しいマルウェアが発見された場合にAppleが取る対応

新しいマルウェアが発見された場合、次のような多くの対策が実行される可能性があります:

- 関連付けられたデベロッパID証明書がある場合は無効になります。
- 公証取り消しチケットがすべてのファイル(アプリおよび関連付けられたファイル)に対して発行されます。
- XProtectシグネチャが作成されリリースされます。

  これらのシグネチャは以前に公証されたソフトウェアにもさかのぼって適用されます。新しいマルウェアが検出されると、以前は可能だった1つまたは複数のアクションが実行できなくなる場合があります。

最後に、マルウェア検出によって一連の対策が開始され、その後の数秒、数時間、あるいは数日にわたって、Macユーザに最高レベルの保護を提供します。

macOSでのアプリからファイルへのアクセスの制御

Appleは、アプリがユーザのデータをどのように扱うかについて、ユーザがすべて理解し、同意し、制御できるべきであると信じています。macOS 10.15ではこのモデルが適用され、ユーザの同意を得てからでなければ、アプリから書類、ダウンロード、デスクトップ、iCloud Drive、およびネットワークボリュームにあるファイルにアクセスできないことがシステムとして保証されます。macOS 10.13以降では、フルストレージデバイスへのアクセスが必要なアプリは、「システム設定」(macOS 13以降)または「システム環境設定」(macOS 12以前)で明示的に追加する必要があります。加えて、アクセシビリティおよびオートメーション機能では、ほかの保護を回避させないために、ユーザの許可が必要になります。アクセスポリシーに応じて、ユーザは以下の場所で設定を変更するように要求される場合があります:

- macOS 13以降の場合:「システム設定」>「プライバシーとセキュリティ」>「プライバシー」
- macOS 12以前の場合:「システム環境設定」>「セキュリティとプライバシー」>「プライバシー」

項目	アプリからユーザへのメッセージ	ユーザがシステムのプライバシー設定を編集しなければならない
アクセシビリティ	✗	✓
フルディスクアクセス	✗	✓
ファイルとフォルダ **注記:** デスクトップ、書類、ダウンロード、ネットワークボリューム、およびリムーバブルボリュームを含みます	✓	✗
オートメーション(Apple Events)	✓	✗

MacでFileVaultをオンにしているユーザは、ブートプロセスを続行し、特化した起動モードへのアクセスを得るために有効な資格情報の入力が必要になります。有効なログイン資格情報や復旧キーがなければ、ボリューム全体は暗号化されたままで、物理ストレージデバイスを取り外して別のコンピュータに接続し直しても、不正アクセスからの保護が維持されます。

エンタープライズ環境では、データを保護するために、IT部門がモバイルデバイス管理(MDM)を使用してFileVaultの構成ポリシーを定義し、適用することが推奨されます。組織が暗号化ボリュームを管理する方法は、組織の復旧キー、個人の復旧キー(オプションでエスクロー用にMDMで保存可能)、それらの組み合わせなど、複数あります。キーローテーションもMDMでポリシーとして設定できます。

メモアプリのセキュリティ機能

メモアプリには、秘密メモの機能が搭載されており(iPhone、iPad、Mac、およびiCloudのWebサイトの場合)、ユーザは特定のメモの内容を保護できます。メモをほかの人と安全に共有することもできます。

秘密メモ

秘密メモはユーザが設定したパスフレーズを使ってエンドツーエンドで暗号化されます。iOS、iPadOS、macOSの各デバイス、およびiCloudのWebサイトでこのメモを見るには、パスフレーズが必要です。iCloudアカウント(「この」デバイスのアカウントを含む)ごとに別々のパスフレーズを設定できます。

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。メモとそのすべての添付ファイルの内容はAES-GCM(AES with Galois/Counter Mode)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、添付ファイル、タグ、および初期化ベクトルが保存されます。新しいレコードが作成されると、元の暗号化されていないデータは削除されます。暗号化に対応する添付ファイルは、イメージ、スケッチ、表、マップ、およびWebサイトです。ほかの種類の添付ファイルを含むメモは暗号化できず、非対応の添付ファイルを秘密メモに追加することもできません。

ユーザが秘密メモを見るには、パスフレーズを入力するかFace IDまたはTouch IDを使って認証する必要があります。秘密メモを表示または作成するときに、ユーザが正しく認証されると、「メモ」は安全なセッションを開始します。安全なセッションが開いている間は、追加の認証なしでほかのメモを見たり保護したりできます。ただし、安全なセッションは、入力された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。異なるパスフレーズで保護されているメモの場合は、認証操作が必要です。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(macOSでは8分)を超えた
- iOSまたはiPadOSデバイスがロックされた

秘密メモのパスフレーズを変更するには、現在のパスフレーズを入力する必要があります。これは、パスフレーズの変更時にはFace IDとTouch IDを利用できないためです。新しいパスフレーズを選択すると、メモアプリは、前のパスフレーズで暗号化されている同じアカウント内のすべての既存メモの鍵を再ラップします。

ユーザがパスフレーズを3回続けて間違って入力するとユーザが設定したヒントが「メモ」に表示されます(設定時にユーザが入力した場合)。ユーザがそれでもパスフレーズを思い出せない場合は、「メモ」の設定でリセットできます。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

パスフレーズでエンドツーエンドの暗号化がなされていないメモは、ほかのユーザと共有できます。共有メモであっても、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は、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。

ショートカットアプリのセキュリティ機能

ショートカットアプリでは、iCloudを使用してAppleデバイス間でショートカットを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。ショートカットは暗号化された形式でローカルに保存されます。

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。ショートカットをインターネットからダウンロードしようとすると、そのショートカットはAppleによるレビューを受けていないという警告がユーザに表示され、そのときにショートカットに関する情報を確認できます。悪質なショートカットから保護するため、実行時に、悪質なショートカッ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。

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から保護するため、前述のマルウェア定義に照らしてJavaScriptが検証されます。ユーザがドメイン上で初めて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。

サービスのセキュリティ

サービスのセキュリティの概要

Appleのデバイスには、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。これらのサービスは、常にユーザのプライバシーとユーザデータのセキュリティを確保しつつ、クラウドストレージ、同期、パスワードストレージ、認証、支払い、メッセージング、通信などのための強力な機能を提供します。

この章では、iCloud、Appleでサインイン、Apple Pay、iMessage、Apple Messages for Business、FaceTime、「探す」、および連係に使用されているセキュリティ技術について扱います。

注記: 一部のAppleのサービスとコンテンツは、国または地域によっては利用できないことがあります。

Apple IDと管理対象Apple ID

Apple IDのセキュリティの概要

Apple IDは、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、Apple IDで以下の条件を満たす強力なパスワードの設定を必須にしています。

- 8文字以上である
- 英字と数字の両方を含んでいる
- 同一文字を3文字以上連続して使用しない
- よく使用されるパスワードではない

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。

また、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、メールとプッシュ通知のいずれかまたは両方でユーザに通知します。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、ユーザ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。

注記: 管理対象Apple IDのパスワードポリシーは、Apple School ManagerまたはApple Business Managerの管理者によって設定されます。

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はデフォルトで**2ファクタ認証**を使用しています。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や、それらの信頼できるデバイスのいずれかまたは信頼できる電話番号からの確認が完了したその他のデバイスでのみ、ユーザのアカウントにアクセスできるようになります。新しいデバイスに初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、iPadOS、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。

ユーザがWebブラウザを使ってAppleのWebサイトにサインインすると、ユーザのiCloudアカウントに関連付けられているすべての信頼できるデバイスに第2要素の要求が送信され、Webセッションの承認が求められます。ユーザが信頼できるデバイスのブラウザからAppleのWebサイトにサインインする場合、確認コードは使用中のデバイスにローカルで表示されます。ユーザがそのデバイスでコードを入力すると、Webセッションが承認されます。

パスワードのリセットとアカウントの復旧

Apple IDアカウントのパスワードを忘れた場合、ユーザは信頼できるデバイスでパスワードをリセットできます。信頼できるデバイスを利用できず、パスワードは分かっている場合、ユーザは信頼できる電話番号を使って、SMS認証を通じて認証できます。また、Apple IDを素早く復旧できるように、以前に使用したことがあるパスコードをSMSと併用してリセットすることができます。これらのオプションのいずれも実行できない場合は、アカウント復旧プロセスに従う必要があります。詳しくは、Appleサポートの記事「Apple IDのパスワードをリセットできない場合にアカウントの復旧機能を使う方法」を参照してください。

管理対象Apple IDのセキュリティ

管理対象Apple IDは、通常のApple IDと同じように機能しますが、企業や教育機関によって所有および管理されます。これらの組織は、パスワードをリセットしたり、FaceTimeやiMessageなどの通信をオフにしたり、従業員、職員、教師、生徒に対する役割に基づくアクセス権を設定したりできます。

管理対象Apple IDでは、一部のサービスは無効になっています(App Store、HomeKit、「探す」など)。

管理対象Apple IDのアクセス管理

組織は、Apple Business Manager、Apple School Manager、およびApple Business Essentialsで利用可能なアクセス管理を使用して、管理対象Apple IDを使用できる場所とそれらが使用できるサービスを定義できます。

アクセス管理を使用すると、ユーザが管理対象Apple IDを使ってどのデバイスでもサインインできるか、管理対象デバイスのみでサインインできるか、または管理対象および監視対象のデバイスのみでサインインできるかを定義できます。また、管理者は、ユーザにWeb上のiCloudへのサインインを許可するかどうかも構成することができます。これにより組織は、デバイスの管理状態を1つの要因として使用して、組織のデータへのアクセス権を付与する必要があるかどうかを決定できます。

さらに、管理者は、ユーザが使用できるiCloudサービスも定義できます。これには、Apple Developer Program、およびAppleSeed for ITベータプログラムへのアクセス権の定義と、Appleプライバシーポータル(privacy.apple.com)へのアクセスをユーザに許可するかどうかの判断も含まれます。

管理対象Apple IDは、Keynote、Numbers、Pages、「リマインダー」、および「メモ」を使用した書類での共同作業と、FaceTimeやiMessageを使用したコミュニケーションにも対応しています。これらのサービスの場合、組織は、ユーザが誰とでも共同作業できるか、Apple School Manager、Apple Business Manager、またはApple Business Essentialsの同じ組織内に作成されたアカウントを持つ人とのみ共同作業できるかを定義できます。

アクセス管理ルールが変更されると、そのルールは、ユーザが自分の管理対象Apple IDでサインインしているデバイスで反映されます。デバイスの管理状態の要件が変更されると、デバイスの状態が新しい要件を満たさない場合、管理対象Apple IDは自動的にデバイスからサインアウトされます。

管理対象Apple IDの調査

Apple School Managerで作成される管理対象Apple IDは、組織が法的規制やプライバシー規制を順守するための**調査機能**にも対応しています。管理者、サイトマネージャ、ユーザマネージャ、または講師の役割を持つユーザは、特定の管理対象Apple IDアカウントを調査できます。

調査担当者が監視できるアカウントは、組織の構成で自分より下位の階層にあるアカウントのみです。例えば、教師は生徒を監視でき、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調査できます。

Apple School Managerを使用して資格情報の調査が要求されると、調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。調査担当者はそのあと、iCloudまたはCloudKit対応アプリ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。調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、調査担当者、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、調査の実行の有無が表示されます。

iCloud

iCloudのセキュリティの概要

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。他社製アプリもiCloudを使って、書類や、デベロッパによって定義されたアプリ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。iCloud DriveなどのiCloudの特定の機能、およびiCloudバックアップは、IT管理者がモバイルデバイス管理(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。

iCloudは強力なセキュリティ方式を使用し、ユーザデータを保護するために厳格なポリシーを採用しています。ほとんどのiCloudデータは、まずデバイスで生成されたiCloudのキーを使用してユーザのデバイス上で暗号化されてから、iCloudサーバにアップロードされます。エンドツーエンドで暗号化されていないデータの場合は、ユーザのデバイスでこれらのiCloudのキーがAppleのデータセンターのiCloudハードウェアセキュリティモジュールに安全にアップロードされます。これにより、Appleはユーザのデータ復旧を支援し、必要なとき(新しいデバイスにサインインするとき、バックアップから復元するとき、またはWeb上のiCloudデータにアクセスするときなど)にいつでもユーザに代わってデータを復号できます。ユーザのデバイスとiCloudサーバ間を移動するデータは、転送時にTLSで個別に暗号化され、iCloudサーバでは、保存時に追加の暗号化レイヤーを使用してユーザデータが保存されます。

暗号鍵は、Appleが利用できる場合はAppleのデータセンターで保護されます。他社のデータセンターに保存されたデータを処理する際、これらの暗号鍵にアクセスするのは、安全なサーバ上で実行されるApple製ソフトウェアのみであり、必要な処理が実行されている間に限られます。プライバシーとセキュリティの強化のために、多くのAppleサービスではエンドツーエンドの暗号化を使用しています。これは、iCloudデータにはユーザ本人のみが、自分のApple IDでサインインした信頼できるデバイスからのみアクセスできることを意味します。

Appleは、iCloudに保存するデータを暗号化して保護するための2つのオプションをユーザに提供しています:

- **標準のデータ保護(デフォルト設定):** ユーザのiCloudデータは暗号化され、暗号鍵はAppleのデータセンターで保護され、Appleはデータとアカウントの復旧を支援できます。特定のiCloudデータ(iCloudキーチェーンのヘルスケアデータとパスワードを含む14のデータカテゴリ)のみがエンドツーエンドで暗号化されます。
- **iCloudの高度なデータ保護:** Appleのクラウドデータの最高レベルのセキュリティを提供するオプションの設定。ユーザが高度なデータ保護をオンにすると、大部分のiCloudのデータの暗号鍵にアクセスできるのはユーザ本人の信頼できるデバイスのみになるため、エンドツーエンドの暗号化によってデータが保護されます。ユーザが高度なデータ保護をオンにすると、エンドツーエンドの暗号化を使用するデータカテゴリの数が23に増え、ユーザのiCloudバックアップ、「写真」、「メモ」などが対象に追加されます。

エンドツーエンドの暗号化で保護されるiCloudデータのカテゴリは、Appleサポートの記事「iCloudのデータセキュリティの概要」に記載されています。

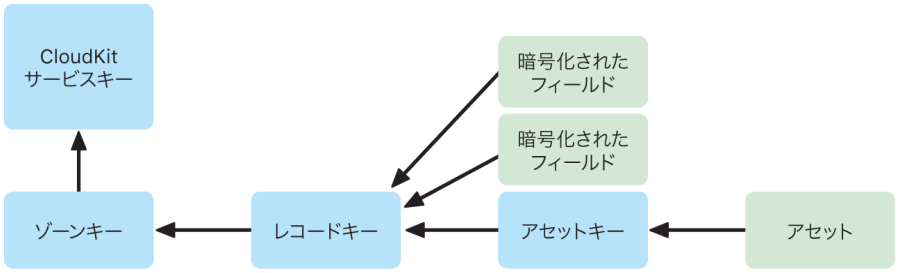
iCloudの暗号化

iCloudでのデータ暗号化はデータストレージモデルと密接に結びついています。これは、アプリとシステムソフトウェアがユーザに代わってiCloudにデータを保存し、デバイスとWeb上にわたるすべてを最新の状態に保つことを可能にするCloudKitフレームワークとAPIから始まります。

CloudKitの暗号化

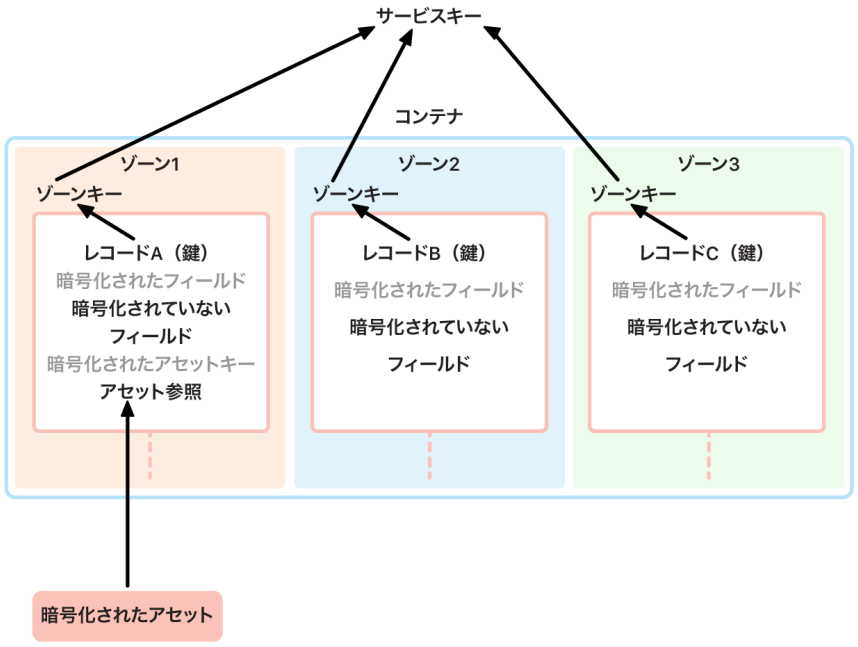
CloudKitはアプリデベロッパがキー値データ、構造化データ、および各種アセット(イメージやビデオなど、データベースとは別に保存された大きなデータ)をiCloudに保存することを可能にするフレームワークです。CloudKitは、コンテナでグループ化された公開データベースと非公開データベースの両方に対応しています。公開データベースはグローバルに共有され、通常は汎用アセットに使用され、暗号化されません。非公開データベースには各ユーザのiCloudデータが格納されます。

CloudKitはデータの構造に一致する鍵の階層を使用します。各コンテナの非公開データベースは、**CloudKitサービスキー**と呼ばれる非対称鍵をルートとする鍵階層によって保護されています。これらのキーは各iCloudユーザに固有であり、信頼できるデバイスで生成されます。データがCloudKitに書き込まれると、すべてのレコードキーがユーザの信頼できるデバイスで生成され、データがアップロードされる前に適切な鍵階層にラップされます。



Appleサポートの記事「iCloudのデータセキュリティの概要」の表に示されている多くのAppleサービスでは、iCloudキーチェーンの同期と同様に保護されたCloudKitサービスキーにより提供される、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、サービスキーはユーザの信頼できるデバイスでのみ使用でき、Appleも他社もアクセスできません。これらのキーは、ユーザがパスワード、パスキー、およびその他のユーザデータを同期するためにiCloudキーチェーンを使用しないことを選択した場合でも、ユーザのデバイス間で同期されます。デバイスを紛失した場合、ユーザは安全なiCloudキーチェーン復元、アカウント復旧用連絡先、またはアカウント復旧キーを使用して、iCloudキーチェーンのデータを復元できます。

暗号鍵の管理



CloudKitの暗号化されたデータのセキュリティは、対応する暗号鍵のセキュリティに依存しています。CloudKitサービスキーは、エンドツーエンドで暗号化されたものと、認証後に使用できるものの2つのカテゴリに分かれています。

- **エンドツーエンドで暗号化されたサービスキー:** エンドツーエンドで暗号化されたiCloudサービスの場合、関連するCloudKitサービスの秘密鍵がAppleのサーバで利用できるようになることはありません。秘密鍵を含むサービスキーのペアは、ユーザの信頼できるデバイス上でローカルに作成され、iCloudキーチェーンのセキュリティを使用してユーザのほかのデバイスに転送されます。iCloudキーチェーンの復元と同期のフローはAppleのサーバによって仲介されますが、暗号化により、Appleのサーバがユーザのキーチェーンデータにアクセスすることはできません。iCloudキーチェーンとそのすべての復旧メカニズムにアクセスできなくなるという最悪のケースでは、CloudKit内のエンドツーエンドで暗号化されたデータが失われます。Appleはこのデータの復旧を支援できません。
- **認証後に使用できるサービスキー:** 「写真」やiCloud Driveなどのその他のサービスでは、サービスキーはAppleのデータセンターのiCloudハードウェアセキュリティモジュールに保存され、Appleの一部のサービスからアクセスできます。ユーザが新しいデバイスでiCloudにサインインし、Apple IDを認証すると、Appleのサーバはそれ以上のユーザの操作や入力なしでこれらのキーにアクセスできるようになります。例えば、iCloud.comにサインインしたあと、ユーザはすぐに自分の写真をオンラインで表示できます。これらのサービスキーは、**認証後に使用できる**キーです。

iCloudの高度なデータ保護

iCloudの高度なデータ保護は、Appleのクラウドデータの最高レベルのセキュリティを提供するオプションの設定です。ユーザが高度なデータ保護をオンにすると、大部分のiCloudのデータの暗号鍵にアクセスできるのはユーザ本人の信頼できるデバイスのみになるため、**エンドツーエンドの暗号化**によってデータが保護されます。高度なデータ保護をオンにしているユーザの場合、エンドツーエンドの暗号化を使用して保護されるデータカテゴリの総数は14から23に増え、iCloudバックアップ、「写真」、「メモ」などが対象に追加されます。

注記: 国や地域によっては、この機能を利用できない場合があります。

高度なデータ保護は、概念的にはシンプルです: デバイスで生成されたあと、Appleのデータセンターの**認証後に使用できる**iCloudハードウェアセキュリティモジュール(HSM)にアップロードされたすべてのCloudKitサービスキーは、それらのHSMから削除され、代わりにアカウントのiCloudキーチェーン保護ドメイン内に完全に保持されます。それらは、既存の**エンドツーエンドで暗号化された**サービスキーのように処理されます。つまり、Appleがこれらのキーを読み取ったりアクセスしたりすることはできません。

高度なデータ保護は、第三者のデベロッパが暗号化済みとしてマークしたCloudKitフィールドとすべてのCloudKitアセットも、自動的に保護します。

高度なデータ保護を有効にする

ユーザが高度なデータ保護をオンにすると、ユーザの信頼できるデバイスは次の2つのアクションを実行します: まず、高度なデータ保護をオンにするというユーザの意図を、エンドツーエンドの暗号化に参加しているほかのデバイスに伝えます。これは、デバイスのローカルのキーで署名された新しい値をiCloudキーチェーンのデバイスメタデータに書き込むことによって行われます。Appleのサーバは、ユーザのほかのデバイスと同期している間、この証明を削除または変更することはできません。

次に、デバイスは**認証後に使用できる**サービスキーをAppleのデータセンターから削除し始めます。これらのキーはiCloud HSMによって保護されているため、この削除は即時かつ永久的で、元に戻すことはできません。キーが削除されると、Appleはユーザのサービスキーによって保護された**すべて**のデータにアクセスできなくなります。この時点で、デバイスは非同期キーのローテーション操作を開始します。これにより、キーが以前にAppleのサーバで利用可能であったサービスごとに新しいサービスキーが作成されます。ネットワークの中断やその他のエラーが原因でキーのローテーションが失敗した場合、デバイスは成功するまでキーのローテーションを再試行します。

サービスキーのローテーションが成功すると、サービスに書き込まれた新しいデータを古いサービスキーで復号することはできなくなります。新しいデータは、ユーザの信頼できるデバイスによってのみ制御され、Appleに提供されたことがない新しいキーで保護されます。

高度なデータ保護とiCloud.comのWebアクセス

ユーザが最初に高度なデータ保護をオンにすると、iCloud.comのデータへのWebアクセスは自動的にオフになります。これは、iCloudのWebサーバが、ユーザのデータを復号して表示するために必要なキーにアクセスできなくなったためです。ユーザは、Webアクセスを再度オンにし、信頼できるデバイスの参加を使用することで、Web上の暗号化されたiCloudデータにアクセスできます。

Webアクセスをオンにしたあと、ユーザは、iCloud.comにアクセスするたびに、信頼できるデバイスのいずれかでWebサインインを承認する必要があります。この承認が、Webアクセスに備えてデバイスを「武装」します。次の1時間の間、このデバイスはAppleの特定のサーバから個々のサービスキーをアップロードする要求を受け入れますが、iCloud.comで通常アクセスできるサービスの許可リストに対応するものだけを受け入れます。つまり、ユーザがWebサインインを承認したあとでも、サーバ要求は、ユーザのデバイスに、iCloud.comでの表示が意図されていないデータ(「ヘルスケア」のデータやiCloudキーチェーンのパスワードなど)のサービスキーをアップロードさせることはできません。Appleのサーバは、ユーザがWeb上でアクセスを要求している特定のデータを復号するために必要なサービスキーのみを要求します。サービスキーは、アップロードされるたびにユーザが承認したWebセッションにバインドされた一時的なキーを使用して暗号化されます。ユーザのデバイスには通知が表示され、データがAppleのサーバで一時的に利用可能になっているiCloudサービスが示されます。

ユーザの選択を保持する

高度なデータ保護とiCloud.comのWebアクセスの設定は、ユーザのみが変更できます。これらの値は、ユーザのiCloudキーチェーンのデバイスメタデータに保存され、ユーザの信頼できるデバイスのいずれかからのみ変更できます。Appleのサーバは、ユーザに代わってこれらの設定を変更したり、以前の構成にロールバックしたりすることはできません。

共有と共同作業のセキュリティへの影響

ほとんどの場合、ユーザがコンテンツを共有して互いに共同作業を行うときに(例えば、共有メモ、共有リマインダー、iCloud Driveの共有フォルダ、iCloud共有写真ライブラリなど)、すべてのユーザが高度なデータ保護をオンにしている場合、Appleのサーバは共有を確立するためだけに使用され、共有データの暗号鍵にはアクセスできません。コンテンツはエンドツーエンドで暗号化されたままになり、参加者の信頼できるデバイスでのみアクセスできます。共有操作ごとに、受信ユーザにプレビューを表示するために、タイトルと代表的なサムネールが標準のデータ保護でAppleによって保存される場合があります。

共同作業を有効にするときに「リンクを知っている人はだれでも」オプションを選択すると、標準のデータ保護の下でAppleのサーバがコンテンツを利用できるようになります。これは、サーバはURLを開くすべての人がアクセスできるようにする必要があるためです。

iWorkの共同作業と「写真」の共有アルバム機能は、高度なデータ保護に対応していません。ユーザがiWork書類で共同作業を行うか、iCloud Driveの共有フォルダからiWork書類を開くと、書類の暗号鍵がAppleのデータセンターのiWorkサーバに安全にアップロードされます。これは、iWorkでのリアルタイムの共同作業では、参加者間の書類の変更を調整するためにサーバ側の仲介が必要になるためです。共有アルバムに追加された写真は、標準のデータ保護で保存されます。この機能により、アルバムをWeb上で公開して共有できるようになります。

高度なデータ保護を無効にする

ユーザは、高度なデータ保護をいつでもオフにすることができます。その場合は、以下のことが行われます:

1.ユーザのデバイスは、まず新しい選択内容をiCloudキーチェーンの参加メタデータに記録します。この設定はすべてのデバイスに安全に同期されます。

2.ユーザのデバイスは、**認証後に使用できる**すべてのサービスのサービスキーをAppleのデータセンターのiCloud HSMに安全にアップロードします。これには、標準のデータ保護の下でエンドツーエンドで暗号化されるサービス(iCloudキーチェーンや「ヘルスケア」など)のキーは含まれません。

デバイスは、高度なデータ保護がオンになる前に生成された元のサービスキーと、ユーザがこの機能をオンにしたあとに生成された新しいサービスキーの両方をアップロードします。これにより、認証後にこれらのサービスのすべてのデータにアクセスできるようになり、アカウントは標準のデータ保護に戻り、ユーザがアカウントにアクセスできなくなった場合に、Appleはユーザがデータの大部分を復旧するための支援を再度行えるようになります。

高度なデータ保護の対象外のiCloudデータ

グローバルなメール、連絡先、およびカレンダーシステムと相互運用する必要があるため、iCloudのメール、連絡先、およびカレンダーはエンドツーエンドで暗号化されません。

高度なデータ保護がオンになっている場合でも、iCloudはユーザ固有のCloudKitサービスキーの保護なしで一部のデータを保存します。CloudKitレコードフィールドは、保護されるコンテナのスキーマで明示的に「暗号化済み」と宣言する必要があり、暗号化されたフィールドの読み取りと書き込みには、専用のAPIを使用する必要があります。ファイルやオブジェクトが変更された日付と時刻は、ユーザの情報を並べ替えるために使用され、ファイルと写真データのチェックサムは、ファイルや写真自体にアクセスしなくても、AppleがユーザのiCloudとデバイスのストレージの重複を排除して最適化できるようにするために使用されます。 特定のデータカテゴリに対して暗号化がどのように使用されるかについて詳しくは、Appleサポートの記事「iCloudのデータセキュリティの概要」を参照してください。

データの重複排除のためのチェックサムの使用(**収束暗号化**と呼ばれるよく知られた手法)などの決定は、iCloudサービスが開始された当初の設計の一部でした。このメタデータは常に暗号化されますが、暗号鍵はAppleによって標準のデータ保護で保存されます。すべてのユーザのセキュリティ保護を引き続き強化するために、Appleでは、高度なデータ保護がオンになっている場合に、この種のメタデータを含むより多くのデータがエンドツーエンドで暗号化されるようにすることに取り組んでいます。

高度なデータ保護の要件

iCloudの高度なデータ保護をオンにするための要件は、次の通りです:

- ユーザのアカウントは、エンドツーエンドの暗号化に対応する必要があります。エンドツーエンドの暗号化には、Apple IDの2ファクタ認証と、信頼できるデバイスに設定されたパスコードまたはパスワードが必要です。詳しくは、Appleサポートの記事「Apple IDの2ファクタ認証」を参照してください。
- ユーザが自分のApple IDでサインインしているデバイスは、iOS 16.2以降、iPadOS 16.2以降、macOS 13.1以降、tvOS 16.2以降、watchOS 9.2以降、および最新バージョンのiCloud for Windowsにアップデートする必要があります。この要件により、以前のバージョンのiOS、iPadOS、macOS、tvOS、またはwatchOSが、誤ってアカウントの状態を修復しようとして、新しく作成されたサービスキーを**認証後に使用できる**HSMに誤って再アップロードすることで誤って処理することを防ぎます。
- ユーザは、自分のアカウントにアクセスできなくなった場合にiCloudデータを復元するために使用できる代替の復旧方法(1つまたは複数の復旧用連絡先または復旧キー)を少なくとも1つ設定する必要があります。

復旧用連絡先の情報が古くなっている場合やユーザがその情報を忘れた場合など、復旧方法が失敗した場合、Appleはユーザのエンドツーエンドで暗号化されたiCloudデータを復元することはできません。

iCloudの高度なデータ保護は、Apple IDに対してのみオンにすることができます。管理対象Apple IDとお子様用アカウント(国または地域によって異なります)には対応していません。

iCloudバックアップのセキュリティ

iCloudは、デバイス設定、アプリデータ、「カメラロール」の写真やビデオ、メッセージアプリでのやり取りといった情報をWi-Fi経由で毎日バックアップします。iCloudバックアップは、デバイスがロックされていて、電源に接続されていて、インターネットにWi-Fiアクセスできる場合にのみ実行されます。iCloudバックアップは、iOSおよびiPadOSで使用するストレージの暗号化に留意して、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できるように設計されています。デフォルトでは、iCloudバックアップのサービスキーはAppleのデータセンターのiCloudハードウェアセキュリティモジュールに安全にバックアップされ、認証後に使用できるデータカテゴリに含まれています。iCloudの高度なデータ保護をオンにしているユーザの場合、iCloudバックアップのサービスキーはエンドツーエンドの暗号化で保護され、信頼できるデバイスのユーザのみが利用できます。

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、元の暗号化された状態でiCloudにファイルがバックアップされます。すべてのファイルが転送中に暗号化され、保管時にはCloudKitの暗号化の説明に記載されているようにアカウントベースの鍵を使って暗号化されます。

iCloudバックアップキーバッグには、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用の非対称(Curve25519)鍵が含まれます。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。

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あと、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バックアップでは以下の内容がバックアップされます:

- 購入した音楽、映画、テレビ番組、アプリ、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デバイスに保存されてい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、App Store、Apple TVアプリ、またはApple Books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、それぞれの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。
- ユーザのデバイス上の写真とビデオ。iOS 8.1、iPadOS 13.1、またはOS X 10.10.3、またはそれ以降でユーザがiCloud写真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、カレンダーの予定、リマインダー、メモ
- デバイス設定
- アプリデータ
- ホーム画面およびアプリの配置
- HomeKitの構成
- メディカルIDのデータ
- ボイスメモのパスワード(必要に応じて、バックアップ中に使用されていた物理SIMカードが必要)
- 「メッセージ」、Apple Messages for Business、テキスト(SMS)、およびMMSメッセージ(必要に応じて、バックアップ時に使用した物理SIMカードが必要)

iCloudバックアップは、デバイスのSecure Enclave UIDのルート暗号鍵から派生したキーで暗号化されたローカルデバイスのキーチェーンのバックアップにも使用されます。このキーはデバイスに固有であり、Appleには知られていません。そのため、データベース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を含むほかの誰も読み出すことはできません。詳しくは、Secure Enclaveを参照してください。

iCloudにメッセージを保管

「iCloudにメッセージを保管」は、ユーザのメッセージ履歴全体を最新の状態に保ち、すべてのデバイスで利用できるようにします。

標準のデータ保護では、iCloudバックアップがオフになっている場合、iCloudに保管されるメッセージはエンドツーエンドで暗号化されます。iCloudバックアップがオンになっている場合、バックアップには「iCloudにメッセージを保管」の暗号鍵のコピーが含まれるため、ユーザがiCloudキーチェーンと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、Appleはユーザがメッセージを復元できるように支援できます。ユーザがiCloudバックアップをオフにすると、今後iCloudに保管されるメッセージを保護するためにデバイスで新しいキーが生成されます。新しいキーはiCloudキーチェーンにのみ保存され、信頼できるデバイスのユーザのみがアクセスできます。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ません。

高度なデータ保護により、iCloudに保管されるメッセージは常にエンドツーエンドで暗号化されます。iCloudバックアップをオンにすると、「iCloudにメッセージを保管」の暗号鍵を含め、その中のすべてがエンドツーエンドで暗号化されます。ユーザが高度なデータ保護をオンにすると、iCloudバックアップのサービスキーと「iCloudにメッセージを保管」コンテナの鍵の両方がローリングされます。詳しくは、Appleサポートの記事「iCloudのデータセキュリティの概要」を参照してください。

iCloudプライベートリレーのセキュリティ

iCloudプライベートリレーは、主にSafariでWebをブラウズしているときにユーザを保護するのに役立ちますが、すべてのDNS名解決リクエストも含まれています。このため、Appleを含め、どの関係者もユーザのIPアドレスとブラウズアクティビティを関連付けることはできません。iCloudプライベートリレーは、複数のプロキシを使用して行われます: Appleが管理するイングレスプロキシと、コンテンツ提供者が管理するイグレスプロキシです。iCloudプライベートリレーを使用するには、ユーザがiOS 15、iPadOS 15、またはmacOS 12.0.1、またはそれ以降を実行していて、Apple IDでiCloud+アカウントにサインインしている必要があります。その場合に、iCloudプライベートリレーは「設定」>「iCloud」または「システム設定」>「iCloud」からオンにできます。

詳しくは、iCloudプライベートリレーの概要を参照してください。

アカウント復旧用連絡先のセキュリティ

ユーザは、高度なデータ保護をオンにしているかどうかに関係なく、信頼する人を最大で5人までアカウント復旧用連絡先として追加して、iCloudアカウントおよびデータ(エンドツーエンドで暗号化されたすべてのデータを含む)の復旧を手伝ってもらうことができます。Appleと復旧用連絡先のいずれも、ユーザのエンドツーエンドで暗号化されたiCloudデータを復元するのに必要な情報を単独で持つことはありません。

復旧用連絡先は、ユーザのプライバシーを考慮して設計されています。ユーザが選択した復旧用連絡先は、Appleには知られていません。Appleのサーバは、ユーザが連絡先に助けを求め、その連絡先が実際に復旧の支援を始めたあと、復旧の試みの後半に復旧用連絡先に関する情報を学習するだけです。その情報は、復旧の完了後は保持されません。

復旧用連絡先のセキュリティプロセス

ユーザがアカウント復旧用連絡先を設定すると、その連絡先と関連付けられた鍵が生成されます。この鍵は、ユーザのiCloudデータ(エンドツーエンドで暗号化されたCloudKitデータを含む)へのアクセスを保護します。次に、ランダムな256ビットのAES鍵が生成され、それを使用して復旧用連絡先の鍵が暗号化され、復旧用連絡先パケットが作成されます。暗号化されたパケットは保管のために復旧用連絡先に送信され、ランダムなAES鍵はAppleに保存されます。AES鍵とパケットのいずれも、基礎となる鍵の情報を単独で提供することはありません。復旧時には、復旧用連絡先からの復旧用連絡先パケットおよびAppleからのAES鍵の両方を取得したのちに、ユーザのデバイスはその2つを組み合わせて元の鍵を復旧し、ユーザのiCloudデータにアクセスすることができます。

ユーザのデバイスは、アカウント復旧用連絡先を設定するために、Appleのサーバと通信して、鍵情報のうちAppleが保持する部分(上記のAES鍵)をアップロードします。さらに、デバイスは復旧用連絡先を使用してエンドツーエンドで暗号化されたCloudKitコンテナを確立し、復旧用連絡先に必要な部分(AES鍵を使用して暗号化された復旧用連絡先パケット)を共有します。また、Appleで作成された認証シークレットも復旧用連絡先と共有されます。これは、アカウントの復旧や、アカウントのパスワードをリセットするのに使用されます。復旧用連絡先を依頼して承認するための通信は、相互認証されたIDSチャネルを通じて行われます。復旧用連絡先が受信した情報は、自動的に復旧用連絡先のiCloudキーチェーンに保存されます。Appleは、CloudKitコンテナの内容にも、この情報が保存されているiCloudキーチェーンにもアクセスできません。共有の実行時にAppleのサーバが参照するのは復旧用連絡先の匿名IDのみです。

そのあと、ユーザがアカウントとiCloudデータを復旧する必要があるときは、復旧用連絡先に協力を依頼できます。すると、復旧用連絡先のデバイスで復旧コードが生成され、復旧用連絡先はそのコードを帯域外でユーザに提供します(直接会って伝える、通話で伝えるなど)。次にユーザは復旧コードをデバイスに入力し、SPAKE2+プロトコルを使用したデバイス間の安全な接続を確立します。Appleはその内容にアクセスできません。このやり取りはAppleのサーバによって進められますが、Appleが復旧プロセスを開始することはできません。

安全な接続が確立され、すべての必要なセキュリティチェックが完了すると、復旧用連絡先のデバイスに保持されている鍵情報の部分と、以前に確立した認証シークレットが、復旧を要求したユーザに返却されます。ユーザはこの認証シークレットをAppleのサーバに提示し、AppleのサーバはAppleが保持している鍵情報へのアクセス権を付与します。認証シークレットの提示により、アカウントのパスワードをリセットして、アカウントへのアクセスを復元することも認証されます。

最後に、ユーザのデバイスはAppleとアカウント復旧用連絡先から受信した鍵情報を再度組み合わせ、それを使用してiCloudデータを復号して復元します。

復旧用連絡先がユーザの同意なく復旧を開始できないように、ユーザのアカウントの生体確認などのセキュリティ機能が採用されています。アカウントがアクティブに使用されている場合、復旧用連絡先を使って復旧するには、デバイスの最新のパスコードまたはiCloudセキュリティコードを知っていることも必要です。

故人アカウント管理連絡先のセキュリティ

ユーザが自分の死後、指定した受取人がユーザのデータにアクセスできるようにしたい場合は、アカウントで故人アカウント管理連絡先を設定できます。故人アカウント管理連絡先は復旧用連絡先とほぼ同様に確立されますが、受取人が使用する鍵情報には、故人のiCloudキーチェーンを復号するのに必要な情報は含まれません。使用される鍵構造はアカウント復旧用連絡先と同様ですが、この場合にはAppleが暗号化パケットを保存し、受取人がAES鍵を保存します。これにより、受取人が受け取る部分を短くして、必要に応じて簡単にプリントできるようにしながらも、同じプロパティを提供することができます。どちらの部分も単独では、基礎となる鍵の情報を提供することはありません。

受取人が受信する鍵情報は、ユーザ向け書類内で「アクセスキー」と呼ばれます。アクセスキーは対応するデバイスに自動的に保存されますが、使用しやすいようにオフラインでプリントや保存をすることも可能です。詳しくは、Appleサポートの記事「Apple IDの故人アカウント管理連絡先を追加する方法」を参照してください。

ユーザの死後、故人アカウント管理連絡先はAppleの請求用Webサイトにサインインしてアクセスを開始します。これには死亡証明書が必要です。このアクセスの一部は、前のセクションで述べた認証シークレットで認証されます。すべてのセキュリティチェックが完了すると、Appleは新しいアカウント用のユーザ名とパスワードを発行し、必要な鍵情報を故人アカウント管理連絡先に渡します。

必要なときにアクセスキーを入力しやすくするために、アクセスキーは英数字コードとそれに関連付けられたQRコードとして参加者に提示されます。入力が済むと、故人のiCloudデータへのアクセスが復元されます。これはデバイス上で実行することも、オンラインでアクセスを確立することもできます。詳しくは、Appleサポートの記事「故人アカウント管理連絡先としてAppleアカウントへのアクセスを申請する」を参照してください。

パスコードとパスワードの管理

パスワードのセキュリティの概要

iOS、iPadOS、およびmacOSでは、パスワードを使用する他社製のアプリやWebサイトでユーザが簡単に認証を行えます。パスワードを管理する最善の方法は、パスワードを使用しなくても済むようにすることです。「Appleでサインイン」を利用すると、ユーザが追加のアカウントやパスワードを作成したり管理したりしなくても、Apple IDの2ファクタ認証でサインインを保護しながら、他社製アプリやWebサイトにサインインできます。「Appleでサインイン」に対応していないサイトでは、強力なパスワードの自動作成機能によって、サイトやアプリ用の強力な一意のパスワードをユーザのデバイスで自動的に作成、同期、および入力できます。iOSおよびiPadOSでは、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」と選択することでユーザが管理できます。

macOSでは、保存済みのパスワードをSafariの「パスワード」環境設定で管理できます。この同期システムは、ユーザが手動で作成したパスワードの同期にも使用できます。

「Appleでサインイン」のセキュリティ

「Appleでサインイン」は、ほかのシングルサインオンシステムに代わる、プライバシーに配慮したサインイン方法です。ワンタップでサインインできる利便性と効率性を実現しながら、ユーザの個人情報の取り扱いについて透明性を確保し、ユーザ自身がコントロールできるようにします。

「Appleでサインイン」では、ユーザがすでに持っているApple IDを使ってアカウントを設定したりアプリやWebサイトにサインインしたりでき、自らの個人情報をより詳細にコントロールできます。アカウントの設定時にアプリから要求できるのはユーザの名前とメールアドレスのみであり、個人のメールアドレスをアプリと共有するか、共有しないで代わりにAppleの新しいプライベートメールリレーサービスを利用するかをユーザが常に選択できます。このメールリレーサービスを利用すると、ユーザの個人アドレスにメールを転送する匿名化された一意のメールアドレスが共有されるため、個人情報のプライバシーとコントロールを保ちながらもデベロッパからの有用な連絡を引き続き受け取ることができます。

「Appleでサインイン」はセキュリティを目的としています。「Appleでサインイン」を利用するすべてのユーザに、Apple IDに対して2ファクタ認証を有効にすることが求められます。2ファクタ認証によって、ユーザのApple IDだけでなく、アプリに登録したアカウントも保護されます。Appleはさらに、プライバシーに配慮した不正防止信号を開発し、「Appleでサインイン」に組み込みました。この信号により、デベロッパは新しいユーザが本物の人間で、Botや不正作成されたアカウントではないことを確認できます。

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、iPadOS、およびmacOS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。iOSおよびiPadOSでは、アプリでも強力なパスワードの自動作成を利用できます。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最新の状態に保たれます。

iOSおよびiPadOS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。

パスワードは、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作成されます。ヒューリスティックでコンテキスト固有のパスワード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、アプリ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。

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、アプリやWebサイトでパスワード規則を提供できます。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。この場合、デバイス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。

パスワードの自動入力のセキュリティ

パスワードの自動入力では、キーチェーンに保存されている資格情報が自動的に入力されます。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。

- アプリや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
- アプリと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

アプリ内でのパスワードの作成および保存と、Apple TVへのパスワードの提供は、iOSおよびiPadOSでのみ可能です。

アプリでのパスワードの自動入力

iOSおよびiPadOSでは、Safariでのパスワードの自動入力の仕組みと同様、保存済みのユーザ名とパスワードをアプリの認証関連フィールドに入力できます。iOSおよびiPadOSで、キーボードのQuickTypeバーに表示される鍵マークをタップします。macOSでは、Mac Catalystを使って構築されたアプリで、認証関連フィールドの下に「パスワード」ドロップダウンメニューが表示されます。

同じapple-app-websiteの関連付けの仕組みを使用するWebサイトや同じapple-app-site-associationファイルを利用するWebサイトとアプリが強固に関連付けられている場合、資格情報のいずれかの領域がパスワード自動入力キーチェーンに保存されていれば、アプリで使用する資格情報の候補がiOSおよびiPadOSのQuickTypeバーとmacOSのドロップダウンメニューに直接表示されます。これにより、それらのアプリに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アプリに提供できるようになります。

パスワードの自動入力では、ユーザが資格情報をアプリに渡すことを承諾するまで、資格情報はアプリに提供されません。資格情報のリストはアプリのプロセスから取得または表示されます。

アプリとWebサイト間に信頼関係がある場合、ユーザがアプリ内から資格情報を送信すると、iOSおよびiPadOSで次回以降利用できるように、それらの資格情報を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。

アプリから保存済みパスワードへのアクセス

iOS、iPadOS、およびmacOSのアプリは、`ASAuthorizationPasswordProvider`および`SecAddSharedWebCredential`を使って、パスワード自動入力キーチェーンによるユーザのサインインの支援を要求できます。パスワードプロバイダとその要求は「Appleでサインイン」と併用できるため、ユーザのアカウントがパスワードベースか「Appleでサインイン」を使って作成されたものかにかかわらず、ユーザがアプリにサインインできるように同じAPIが呼び出されます。

アプリが保存済みパスワードにアクセスできるのは、アプリのデベロッパと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だけです。アプリのデベロッパはアプリ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が承認したアプリの一意のアプリ識別情報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アプリがインストールされると、iOSおよびiPadOS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アプリのアプリ識別情報がファイルのリストにある場合は、iOSおよびiPadOSによってそのWebサイトとアプリが信頼関係にあるとマークされます。信頼関係ある場合にのみ、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、パスワードをアプリに渡したり、アップデートまたは削除したりすることはできません。

パスワードのセキュリティに関する勧告

iOS、iPadOS、およびmacOSのパスワード自動入力のパスワードリストでは、ユーザの保存済みパスワードのうち、ほかのWebサイトで**再利用**されるものと、安全性が**低い**と見なされるパスワード、および**データ漏えい**によって侵害されたことのあるパスワードが示されます。

概要

複数のサービスで同じパスワードを使うと、それらのアカウントがクレデンシャルスタッフィング攻撃に対して脆弱になる可能性があります。いずれかのサービスが侵害されてパスワードが漏えいすると、攻撃者がほかのサービスでも同じ資格情報を試すことで、ほかのアカウントも不正使用されるおそれがあります。

- パスワードがさまざまなドメイン間で複数の保存済みパスワードとして使用されていることが認められると、そのパスワードには**再利用**とマークが付けられます。
- 攻撃者がパスワードを容易に推測できる場合、そのパスワードは**安全性が低い**としてマークされます。iOS、iPadOS、およびmacOSでは、辞書にある単語の使用、よくある文字の置き換え（「password」の代わりに「p4ssw0rd」など）、キーボードによるパターン（QWERTYキーボードでの「q12we34r」など）、繰り返しのシーケンス（「123123」など）のような、覚えやすいパスワードを作成するためによく使用されるパターンが検出されます。これらのパターンは多くの場合サービスでのパスワードの最小要件を満たすために使用されますが、パスワードの総当たり（ブルートフォース）攻撃を利用してパスワードの入手を試みる攻撃者がよく使用するものでもあります。

  多くのサービスで4桁または6桁のPINコードが明確に要求されるため、それらの短いパスコードは別のルールで評価されます。数字の昇順または降順（「1234」や「8765」など）という非常によく使われるPINコードや、繰り返しのパターン（「123123」や「123321」など）の場合は、安全性が低いPINコードと見なされます。
- パスワードの監視機能によりデータ漏えいに含まれていたと断言できる場合、パスワードには**漏えい**とマークが付けられています。詳しくは、パスワードの監視を参照してください。

安全性が低いパスワード、再利用されたパスワード、漏えいしたパスワードは、パスワードのリストに表示されるか（macOS）、専用の「セキュリティに関する勧告」インターフェイスで見られます（iOSおよびiPadOS）。ユーザが以前に保存した、非常に安全性が低いパスワードやデータ漏えいによって侵害されたことのあるパスワードを使ってSafariでWebサイトにログインすると、強力なパスワードの自動作成によって新しいパスワードにアップグレードすることを強くすすめる通知が表示されます。

iOSおよびiPadOSでのアカウント認証のセキュリティをアップグレードする

（Authentication Servicesフレームワークで）Account Authentication Modification Extensionを実装するアプリは、ボタンをタップするだけで簡単にパスワードベースのアカウントをアップグレードできます。つまり、「Appleでサインイン」または強力なパスワードの自動作成の使用に切り替えることができます。この拡張ポイントはiOSおよびiPadOSで利用できます。

アプリがこの拡張ポイントを実装済みで、デバイスにインストールされている場合は、ユーザが「設定」のiCloudキーチェーンのパスワードマネージャでアプリに関連付けられた資格情報の「セキュリティに関する勧告」を表示すると、機能拡張のアップグレードのオプションが表示されます。アップグレードは、ユーザが危険にさらされている資格情報でアプリにサインインするときにも提供されます。アプリは、サインイン後にアップグレードオプションでユーザにメッセージが表示されないようシステムに通知する機能があります。新しいAuthenticationServices APIを使用すると、アプリは、理想的にはアプリのアカウント設定またはアカウント管理画面から、機能拡張を呼び出して、それ自体でアップグレードを実行することもできます。

アプリは、強力なパスワードのアップグレード、「Appleでサインイン」のアップグレード、またはその両方に対応することを選択できます。強力なパスワードのアップグレードでは、システムにより自動的に「強力なパスワードの自動作成」が生成されます。必要に応じて、アプリは、新しいパスワードの生成時に従うべきカスタムのパスワード規則を提供できます。ユーザがアカウントをパスワードの使用から「Appleでサインイン」の使用に切り替えると、システムは、アカウントを関連付ける機能拡張に新しい「Appleでサインイン」資格情報を提供します。ユーザのApple IDメールは、資格情報の一部として提供されません。「Appleでサインイン」のアップグレードが正常に完了すると、システムは、以前に使用したパスワード資格情報がユーザのキーチェーンに保存されている場合はそこから削除します。

Account Authentication Modification Extensionには、アップグレードを実行する前に追加のユーザ認証を実行する機会があります。パスワードマネージャ内で、またはアプリにサインインしたあとに開始されたアップグレードでは、機能拡張によりアップグレードするアカウントのユーザ名とパスワードが入力されます。アプリ内のアップグレードの場合は、ユーザ名のみが入力されます。機能拡張がさらにユーザ認証を必要とする場合は、アップグレードに対処する前にカスタムのユーザインターフェイスを表示するよう要求できます。このユーザインターフェイスを表示することを目的としたユースケースは、アップグレードを承認するためにユーザに認証の2番目の要素を入力してもらうことです。

パスワードの監視

パスワードの監視は、ユーザのパスワード自動入力キーチェーンに保存されているパスワードを、さまざまなオンライン組織からの漏えいで公開されたことが分かっているパスワードの、継続的にアップデートされキュレートされたリストと照合する機能です。この機能がオンになっている場合、監視用プロトコルは、ユーザのパスワード自動入力キーチェーンのパスワードをキュレートされたリストに対して継続的に照合します。

監視の仕組み

ユーザのデバイスは、ユーザのパスワードに対してラウンドロビンチェックを継続的に実行し、ユーザのパスワードやパスワードマネージャの使用パターンに依存しない間隔でクエリを実行します。これにより、漏えいしたパスワードの最新のキュレートされたリストで検証の状態が最新の状態に保たれます。ユーザが持っている一意のパスワードの数に関連する情報の漏えいを防ぐために、要求はバッチ処理され、並行して実行されます。各チェックで一定数のパスワードが並行して検証され、ユーザが持っている数がこの数より少ない場合は、ランダムなパスワードが生成され、差を補うためにクエリに追加されます。

パスワードの照合の仕組み

パスワードは2つのパートから成るプロセスで照合されます。最も漏えいすることの多いパスワードは、ユーザのデバイスのローカルリスト内に含まれています。ユーザのパスワードがこのリストに含まれると、外部の操作なしでユーザにすぐに通知されます。これは、ユーザが持っているパスワードのうち、パスワードの侵害によって最も危険にさらされているものの情報が漏えいすることを防止するためです。

パスワードが最も頻度の高いリストに含まれていない場合、そのパスワードは、漏えいした頻度の低いパスワードと照合されます。

ユーザのパスワードをキュレートされたリストと比較する

ローカルリストに存在しないパスワードが一致するかどうかを検証するには、Appleサーバとのやりとりが必要です。正当なユーザのパスワードがAppleに送信されないようにするために、ユーザのパスワードを漏えいした大量のパスワードと比較する、暗号の**秘匿共通集合計算**が展開されます。これは、侵害される危険性が低いパスワードについて、Appleと共有される情報をほぼなくすためです。ユーザのパスワードについては、この情報は暗号学的ハッシュの15ビットプレフィックスに限定されます。最も漏えいされることの多いパスワードのローカルリストを使用して、この対話型プロセスから最も頻繁に漏えいされるパスワードを削除すると、Webサービスのバケット内のパスワードの相対頻度の差が減少するため、これらの探索からユーザパスワードを推測することは実現困難になります。

基礎となるプロトコルは、本書の執筆時点で約15億のパスワードが含まれていたキュレートされたパスワードのリストを、2^{15}の異なるバケットに分割します。パスワードが属するバケットは、パスワードのSHA256ハッシュ値の最初の15ビットに基づいています。さらに、漏えいした各パスワード、pwは、NIST P256曲線上の楕円曲線の点に関連付けられています: $P_{pw} = \alpha \cdot H_{SWU}(pw)$。ここで、αはAppleだけが知っているランダムな秘密鍵であり、H_{SWU}は、パスワードをShallue-van de Woestijne-Ulas方式に基づいて曲線の点にマッピングするランダムなoracle関数です。この変換はパスワードの値を計算によって隠すように設計されており、パスワードの監視を使用して、新たに漏えいしたパスワードが公開されるのを防ぎます。

秘匿共通集合計算を行うために、ユーザのデバイスは、SHA256(upw)の15ビットプレフィックスであるλ(upwはユーザのパスワードの1つ)を使用して、ユーザのパスワードが属するバケットを決定します。デバイスは独自のランダム定数βを生成し、$P_c = \beta \cdot H_{SWU}(upw)$を、λに対応するバケットの要求と共にサーバに送信します。ここで、βはユーザのパスワードに関する情報を隠し、パスワードからAppleに公開される情報をλに制限します。最後に、サーバはユーザのデバイスから送信された点を取得し、$\alpha P_c = \alpha\beta \cdot H_{SWU}(upw)$を計算して、それを点の適切なバケット、$B\lambda = \{ P_{pw} \mid$ SHA256(pw)はプレフィックスλで始まる}と共にデバイスに返します。

返された情報により、デバイスは、$B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$を計算でき、$\alpha P_c \in B'_\lambda$の場合はユーザのパスワードが漏えいしたことがあることを確かめます。

ほかのユーザまたはAppleデバイスへのパスワード送信

Appleは、ほかのユーザまたはAppleデバイスに、AirDropおよびApple TVでパスワードを安全に送信します。

AirDropを使って別のデバイスに資格情報を保存する

iCloudを有効にすると、ユーザはAirDropを使って保存済みの資格情報をほかのデバイスに送信できます。資格情報には、ユーザ名、パスワード、対象Webサイトが含まれます。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。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のアプリで資格情報を入力する

Apple TVのアプリ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またはiPad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。この暗号化方式は次のように確立されます:

- デバイスとApple TVが同じiCloudアカウントを使用している場合は、デバイス間の通信の暗号化が自動的に行われます。
- デバイスがApple TVで使用されているものとは異なるiCloudアカウントにサインインしている場合、ユーザはPINコードを使用して暗号化接続を確立するよう求められます。このメッセージを受信するには、デバイスのロックを解除し、Apple TVとペアリングされたSiri Remoteにデバイスを近付ける必要があります。

BLE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、アプリ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

iOS、iPadOS、macOSでは、ユーザが連携可能な他社製アプリを「パスワードの自動入力」の資格情報プロバイダに指定することができます。この設定は、「パスワード」設定（iOSおよびiPadOS）、「システム設定」（macOS 13以降）または「システム環境設定」（macOS 12以前）の「機能拡張」設定で行うことができます。これはアプリ機能拡張を利用したメカニズムです。資格情報プロバイダ機能拡張では、資格情報を選択する表示を**提供する必要があります**。また、機能拡張では、保存された資格情報のメタデータを**提供する場合もあり**、QuickTypeバー（iOSおよびiPadOS）またはオートコンプリート候補（macOS）で直接使えるようにすることができます。メタデータには、資格情報の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。ユーザが資格情報をアプリまたはSafariのWebサイトに自動入力することを選択すると、iOS、iPadOS、macOSは機能拡張と通信してパスワードを取得します。資格情報のメタデータは、クレデンシャルプロバイダのアプリのコンテナ内に保存され、アプリのアンインストール時に自動的に削除されます。

iCloudキーチェーン

iCloudキーチェーンのセキュリティの概要

iCloudキーチェーンでは、ユーザがiPhone、iPadデバイスやMacコンピュータの間でパスワードとパスキーを安全に同期しつつ、Appleに対しては公開しないように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のその他の目標は、使いやすさと、ユーザのすべてのデバイスでアクセスできないときでもキーチェーンの内容を復元できることです。iCloudキーチェーンは、キーチェーンの同期とキーチェーン復元の2つのサービスで構成されています。

iCloudキーチェーンとキーチェーン復旧は、ユーザのパスワードとパスキーが、以下の状況でも保護されるように設計されています:

- 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。

パスワードマネージャとiCloudキーチェーンの統合

iOS、iPadOS、およびmacOSでは、Safariでアカウントパスワードとして使用するための暗号化された強力でランダムな文字列を、自動的に生成できます。iOSとiPadOSでは、アプリ用の強力なパスワードを生成することもできます。生成されたパスワード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エンドツーエンドで暗号化されます。

キーチェーンの安全な同期

ユーザがiCloudキーチェーンを2ファクタ認証アカウントで初めて有効にすると、デバイス自身が同期識別情報を確立および作成します。同期識別情報は楕円曲線の非対称鍵（P-384を使用）から構成され、デバイスのキーチェーンに保存されます。各デバイスはユーザのほかのデバイスの同期識別情報のリストを独自に保持しており、このリストにID鍵のうちの1つを使用して署名します。これらのリストはCloudKitに保存されるため、ユーザのデバイス間でキーチェーンデータを安全に同期する方法について、ユーザのデバイスが合意に達することができます。

古いiCloudデバイスとの互換性については、同様の信頼できる同期グループが作成され、別の同期識別情報が形成されます。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。

同期グループのiCloud保管

2ファクタ認証が有効なアカウントでは、各デバイスの信頼できるデバイスのリストがCloudKitに保存されます。このリストの読み出しにはユーザのiCloudパスワードが必要であり、所有デバイスの秘密鍵がないと変更を加えられません。

同様に、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保存されます。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。

ユーザのほかのデバイスが同期グループに追加される仕組み

新しいデバイスがiCloudにサインインすると、既存のiCloudキーチェーンデバイスとペアリングしてそのデバイスからスポンサー認証されるか、iCloudキーチェーン復旧を使用することで、iCloudキーチェーンの同期グループに参加します。

ペアリングフロー中、(2ファクタ認証が有効なアカウントでは)申請者デバイスは同期グループと同期リストの両方に対して新しい同期識別情報を作成し、それらをスポンサーに提示します。スポンサーは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。2ファクタ認証が有効なアカウントでは、ID鍵で署名された**バウチャー**もスポンサーデバイスから参加デバイスに提供され、申請者デバイスは信頼していいことが示されます。そして、申請者デバイスを含めるように、信頼する同期識別情報の個別リストがアップデートされます。

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。状況に応じて、メンバー同士でCloudKitまたは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ます。両方のグループメンバーが同じ項目に対するアップデートを所有している場合は、一方が選択され、最終的な整合性が取られます。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参加すると、この「参加プロセス」が繰り返されます。例えば、次のデバイスが参加すると、既存のデバイスのいずれかとペアリングできます。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ます。これは、すべてのメンバーのキーチェーン項目を同じ内容にするためです。

特定の項目のみを同期

iMessageキーなどの一部のキーチェーン項目はデバイス固有であり、そのデバイスで留まっている必要があります。予期しないデータ転送を防ぐために、同期するすべての項目は`kSecAttrSynchronizable`属性で明示的にマークされる必要があります。

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パスワードやHomeKitの暗号鍵などのエンドツーエンドiCloud暗号化に対応したキーチェーン項目にこの属性を設定します。

また、デフォルトでは、他社製アプリ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`属性を設定する必要があります。

安全なiCloudキーチェーン復元

iCloudキーチェーンは、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、キーチェーンをAppleにエスクロー(預託)します。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またはパスキー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。

二次認証を使用する

強力なパスコードを確立する方法は複数あります:

- 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る場合、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。

キーチェーンのエスクロープロセス

パスコードが確立されると、キーチェーンがAppleにエスクローされます。iOS、iPadOS、またはmacOSデバイスは、まずユーザのキーチェーンのコピーを書き出したあと、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。2ファクタ認証が有効なアカウントの場合、キーチェーンはCloudKitにも保存され、iCloudエスクローレコードの内容でのみ復元可能な中間キーにラップされるため、同じレベルの保護が提供されます。

また、エスクローレコードの内容によって、復旧中のデバイスがiCloudキーチェーンに再度参加することが許可され、復旧中のデバイスがエスクロープロセスを正常に実行したため、アカウントのオーナーによって認証されたことが既存のデバイスに証明されます。

注記: セキュリティコードの確立に加えて、ユーザはiCloudアカウントに電話番号を登録する必要があります。これにより、キーチェーン復元中に二次認証が提供されます。ユーザはSMSメッセージを受信します。復元を続行するためには、これに返信する必要があります。

iCloudキーチェーン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(ハードウェアセキュリティモジュール)のクラスタです。前述の通り、クラスタごとに鍵があり、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。そのあと、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、デバイスがエスクローデータを使用して、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、CloudKitと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。エスクローサービスは、エスクローレコードの認証と取得の試行を10回のみ許可します。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。

Apple Pay

Apple Payのセキュリティの概要

Apple Payを使えば、サポートされているiPhone、iPad、Mac、およびApple Watchの各デバイスで、プライバシーを守りながら、店舗やアプリ内、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。ユーザは、Apple Pay対応の交通系ICカード、学生証、アクセスカードをAppleウォレット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のコンポーネントのセキュリティ

Apple Payは、安全かつ確実に買い物できるようにするいくつかのハードウェア機能とセキュリティ機能を使用します。

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。Secure Element ICとJava Cardプラットフォームは、EMVCoのセキュリティ評価プロセスに従って認定されます。セキュリティ評価が正常に完了すると、EMVCoから専用のICおよびプラットフォーム証明書が発行されます。

Secure Element ICは、コモンクライテリア規格に基づいて認証されています。

NFCコントローラ

NFCコントローラは、Near Field Communication（NFC）プロトコルに対応し、アプリケーションプロセッサとSecure Element間、およびSecure ElementとPOS端末間の通信をルーティングします。

Appleウォレット

Appleウォレットアプリは、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Appleウォレット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およびiPadOSの設定アシスタントと「設定」
- Apple Watch用のWatchアプリ
- Touch IDを搭載したMacコンピュータの「システム設定」（macOS 13以降）または「システム環境設定」（macOS 12以前）の「ウォレットとApple Pay」

また、Appleウォレットに交通系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、アクセスカードなどを追加して管理することもできます。

Secure Enclave

iPhone、iPad、Apple Watch、Touch IDを搭載したMacコンピュータ、およびTouch ID搭載Magic Keyboardを使用するAppleシリコン搭載Macコンピュータでは、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、Appleウォレットで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、アクセスカードの設定やプロビジョニングを管理します。また、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、アプリ内やWeb上での支払いに使用する支払い資格情報の再暗号化もApple Payサーバが行います。

Apple Payがユーザの購入を保護する方法

Secure Element

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。

NFCコントローラ

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Face ID、Touch 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、アプリ内および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、およびプリペイドカード

カードのプロビジョニングのセキュリティの概要

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Appleウォレットに追加すると、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(通常はペイメントネットワーク)に安全に送信されます。カード発行会社(またはそのサービスプロバイダ)はこの情報を使って、そのカードのAppleウォレット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、以下の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ペイメントネットワークとデータの送受信を行います:

- Required Fields
- Check Card
- Link and Provision

カード発行会社またはペイメントネットワークはこれらの呼び出しを使用して、カード発行会社がカードの確認、承認、およびAppleウォレットへの追加を行えるようにします。これらのクライアント/サーバセッションでは、TLS 1.2を使用してデータが転送されます。

完全なカード番号は、デバイスにもApple Pay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、暗号化されたあとに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、ほとんど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がApple Pay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なく、iOS、iPadOS、およびwatchOSの各デバイスから、およびTouch IDを搭載したMacコンピュータと、Touch IDを搭載したMagic Keyboardを使用するAppleシリコン搭載Macコンピュータから切り離されています。

Apple Watchで使用するカードをApple Payに登録するには、iPhoneのApple Watchアプリまたはカード発行会社が提供するiPhone アプリを使用します。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Apple Payに追加する

Appleデバイスではクレジットカードを手動でApple Payに追加できます。

クレジットカードまたはデビットカードを手動で追加する

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」、Appleウォレット、またはApple Watchアプリで、デバイスのカメラを使用して撮影することでそれらの情報を入力できます。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。その後、情報が暗号化されて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。ユーザが発行会社の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、(a)ユーザの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）、(b)ユーザの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Appleデバイスなど）、(c)ユーザがカードを追加したときのおおよその位置情報（ユーザが「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Appleウォレット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、カードのデザインと、連絡先情報、関連するカード発行会社のアプリ、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、カード発行会社の利用規約がダウンロードされてデバイスに表示されます。そのあと、利用規約の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。

カード発行会社のアプリ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

アプリでApple Payを使用できるよう登録されている場合は、そのアプリ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。これは、Appleデバイスがカード情報を読み取れないようにするためです。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。

カード発行会社のWebサイト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

一部のカード発行会社は、Appleウォレットのカードプロビジョニングプロセスをそのサイトから直接開始する機能を提供しています。この場合、ユーザは、カード発行会社のWebサイトでプロビジョニングするカードを選択することでタスクを開始します。次にユーザは自己完結型のAppleサインインエクスペリエンス（Appleのドメイン内のみで処理されます）にリダイレクトされ、Apple IDでサインインするように求められます。サインインに成功すると、次にユーザはカードをプロビジョニングする1つ以上のデバイスを選択して、プロビジョニング結果を各ターゲットデバイス上で確認するように求められます。

追加の検証を追加する

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、承認された他社製アプリ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、ユーザには、カード発行会社にすでに登録されている連絡先情報から選択するオプションが表示されます。そこにコードが送信されるので、そのコードをAppleウォレット、「設定」、またはApple Watchアプリに入力する必要があります。カスタマーサービスやアプリ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。

Apple Payでの支払い承認

Secure Enclaveが搭載されたデバイスでは、Secure Enclaveから承認を受けたあとにのみ支払いを行うことができます。この際、iPhone、iPad、またはTouch IDを搭載したMac（あるいはTouch ID搭載Magic Keyboardとペアリングされているmac）では、ユーザが生体認証あるいはデバイスパスコードまたはパスワードで認証したことを確認します。利用できる場合には生体認証がデフォルトの方法ですが、パスコードまたはパスワードもいつでも使用できます。また、指紋の認証に3回失敗するか、（iPhoneまたはiPadで）顔の認証に2回失敗すると、自動的にパスコードまたはパスワードが使用できるようになります。5回失敗すると、パスコードまたはパスワードが必須になります。生体認証が設定されていない場合や、Apple Payに対して有効になっていない場合にも、パスコードまたはパスワ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。

共有ペアリングキーを使用する

Secure EnclaveおよびSecure Elementは、シリアルインターフェイスを経由して通信します。これには、AESに基づいた暗号化と認証が使用され、リプレイ攻撃から保護するためにアンチリプレイ値が使われます。両者は直接接続されてはいませんが、製造工程でプロビジョニングされた共有ペアリング鍵を使用して安全に通信します。そのプロビジョニングプロセスでは、Secure Enclaveが、自身のUID鍵およびSecure Elementの一意識別子からペアリング鍵を生成します。次にSecure Enclaveは、ペアリング鍵を工場のハードウェアセキュリティモジュール（HSM）に安全に転送します。そして、HSMがペアリング鍵をSecure Elementに導入します。

安全なトランザクションを承認する

ユーザがトランザクションを承認すると(Secure Enclaveと直接通信する物理ジェスチャを含む)、認証の種類およびトランザクションの種類(非接触型またはアプリ内)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値は、ユーザが初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、ペアリングキーを利用して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終了済みのマークを付けます。

動的なセキュリティに支払い用クリプトグラムを使用する

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、トランザクションカウンタと鍵を使って計算されます。トランザクションカウンタは、新しいトランザクションが発生するたびに増分されます。鍵は、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、ペイメントネットワークとカード発行会社のいずれかまたは両方に通知されます。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:

- 端末が生成する予測不可能な数(NFC(Near-Field-Communication)トランザクションの場合)
- Apple Payサーバのアンチリプレイ値(アプリ内トランザクションの場合)
- CVM(Cardholder Verification Method)情報などのユーザ検証の結果

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るため、発行会社が各トランザクションの検証に使用できます。セキュリティコードの長さは、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。

Apple Payを使ってカードで支払う

Apple Payを使って、店舗、アプリ内、およびWebサイトで購入したものの代金を支払うことができます。

店舗でカードで支払う

動作中のiPhoneまたはApple Watch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、Appleウォレット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、以下の操作を行えます:

- 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
- 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
- ロック画面からApple Payを許可するアクセシビリティ機能を使用する

次に、ユーザがFace ID、Touch 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、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。

アプリ内でカードで支払う

Apple Payは、iOS、iPadOS、macOS、およびwatchOSのアプリでの支払いにも使用できます。ユーザがApple Payを利用してアプリ内で支払うと、Appleは、暗号化されたトランザクション情報を受信して、デベロッパまたは加盟店にルーティングします。Appleはデベロッパ固有の鍵を使ってトランザクションを再暗号化してから、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。

アプリが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トランザクションを再暗号化したあと、加盟店に転送します。

アプリが支払いを要求する場合、そのアプリは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。アプリは、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。次にアプリは、Apple Payシートの表示をiOS、iPadOS、macOS、またはwathOSに依頼します。Apple Payシートは、アプリの情報と、必要なその他の情報（使用するカードなど）を、iOS、iPadOS、またはwatchOSに要求します。

この時点でアプリには、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アプリに提供されるのは、ユーザがFace ID、Touch ID、またはデバイスパスコードで支払いを承認したあとです。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。

App Clip内でカードで支払う

App Clipは、そのアプリのごく一部の機能を提供して、完全なアプリをダウンロードしなくても、自転車を借りたり駐車場代を支払ったりといったタスクをユーザが素早く実行できるようにします。App Clipが支払いに対応している場合、ユーザは「Appleでサインイン」を使用してから、Apple Payを使用して支払いを行うことができます。ユーザがApp Clip内から支払いを行うと、すべてのセキュリティおよびプライバシー対策はアプリ内での支払いの場合と同じになります。

アプリ支払いをユーザが承認し、加盟店が検証する方法

ユーザと加盟店は、安全なアプリ支払いのために、Appleサーバ、Secure Element、デバイス、アプリのAPIに情報を渡します。まず、ユーザがアプリ支払いを承認すると、アプリはApple Payサーバを呼び出してアンチリプレイ値を取得します。サーバはこの値とほかのトランザクションデータをSecure Elementに送信します。そこで支払い資格情報が計算され、Appleの鍵を使用して暗号化されます。次に、Secure Elementは支払い資格情報をApple Payサーバに戻します。Apple Payサーバは資格情報を復号し、そのアンチリプレイ値とApple Payサーバからあらかじめ送信されたアンチリプレイ値とを照合してから、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。そして、Appleのサーバが支払いをデバイスに戻し、デバイスは支払いをアプリのAPIに戻し、APIは処理のために支払いを加盟店のシステムに渡します。加盟店は支払い資格情報を復号し、それがトランザクションの正しい受信者であることを検証します。

APIには、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、アプリで注文番号や顧客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、アプリデベロッパが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サイトでカードで支払う

Apple Payは、iPhone、iPad、Apple Watch、およびTouch IDを搭載したMacコンピュータから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に対応するすべてのWebサイトが、Appleに登録する必要があります。ドメインの登録後は、AppleがTLSクライアント証明書を発行したあとでのみドメイン名検証が実行されます。Apple Payをサポートするサイトは、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、iPhone、iPad、およびMacの各デバイスの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、すべてのプライバシーおよびセキュリティ対策はアプリ内での支払いの場合と同じになります。

ユーザがMacからiPhoneまたはApple Watchに支払い関連の情報を送信する場合、Apple PayのHandoffで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がユーザのMacから認証側デバイスに転送されます。MacのIDSクライアント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の識別情報が含まれます。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Face ID、Touch 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（BLE）アドバタイズメントを通じて判定されます。

自動支払いと加盟店トークン

iOS 16以降では、Apple Payを提供するアプリやWebサイトは、ユーザのデバイス間で常に安全な支払いを可能にするApple Payの加盟店トークンを活用できます。iOS 16のアップデートされたApple Pay支払いシートは、事前に承認した支払い操作の最適化も行います。Apple Pay APIの新しいトランザクションタイプにより、アプリとWebサイトのデベロッパは、サブスクリプション、定期的請求、分割払い、およびカード残高の自動チャージの支払いシートの操作を微調整することができます。

加盟店トークンはデバイス固有ではないため、ユーザがデバイスから支払い用カードを削除した場合でも、定期的支払いの継続を可能にします。

複数の加盟店への支払い

iOS 16以降では、Apple Payには、1つのApple Pay支払いシート内に複数の加盟店での購入金額を明記する機能が組み込まれています。これによって顧客は、航空券、レンタカー、ホテルを含む旅行パッケージを一括購入し、あとで個々の加盟店に送金するといった柔軟な支払いが可能になります。

Apple Payの非接触型パス

対応パスから対応NFC端末にデータを送信する場合、AppleはApple VAS（Value Added Service）プロトコルを使用します。VASプロトコルは非接触型端末またはiPhoneのアプリに実装でき、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。ユーザがパスプロバイダの識別情報を含むパスを持っている場合、ユーザはFace ID、Touch 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鍵がパスプロバイダ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。

iOS 12.0.1からiOS 13までは、加盟店のNFC端末にパスを提示する前にユーザが手動でパスを選択できます。iOS 13.1以降では、選択されたパスで、ユーザ認証を要求するか、認証なしで使用できるようにするかをパスプロバイダが手動で設定できます。

カードをApple Payで使用不可にする

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とAR（Authorization Random）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。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終了済みのマークを付けます。これにより以下のような状況の場合に、オペレーティングシステムから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。

状況	デバイス
パスコードがオフになっている。	iPhone、iPad、Apple Watch
パスワードがオフになっている。	Mac
ユーザがiCloudからサインアウトした。	iPhone、iPad、Mac、Apple Watch
ユーザが「すべてのコンテンツと設定を消去」を選択した。	iPhone、iPad、Mac、Apple Watch
デバイスがリカバリモードから復元された。	iPhone、iPad、Mac、Apple Watch
ペアリングが解除された	Apple Watch

カードの一時停止、削除、消去

ユーザは、「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、「探す」やiCloud.comを使用して、またはAppleウォレット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Apple Watchアプリ、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。

ユーザが「すべてのコンテンツと設定を消去」または「探す」を使用して、あるいはデバイスを復元することでデバイス全体を消去すると、iPhone、iPad、Mac、およびApple WatchはSecure Elementに対して、すべてのカードに終了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。

Apple Cardのセキュリティ

対応する機種のiPhoneおよびMacでは、ユーザが安全にApple Cardに入会を申し込むことができます。

Apple Cardの申し込み

iOS 12.4以降、macOS 10.14.6以降、およびwatchOS 5.3以降では、Apple CardをApple Payで使用して、店舗、アプリ、Web上での支払いも行えます。

Apple Cardに入会を申し込むには、ユーザがApple Pay対応のiPhoneまたはiPad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。または、Apple IDでサインインしたあとでapply.applecard.appleで申し込むことができます。申し込みが承認されると、ユーザが自分のApple IDでサインインしているすべてのApple Pay対応デバイスのAppleウォレット、または「設定」>「ウォレットとApple Pay」でApple Cardを使用できるようになります。

ユーザがApple Cardに入会を申し込むと、ユーザの識別情報がAppleのIDプロバイダパートナーによって安全に確認されたあと、識別と信用評価のためにGoldman Sachs Bank USAと共有されます。

申し込み時に提供された社会保障番号やID書類のイメージなどの情報は、AppleのIDプロバイダパートナーとGoldman Sachs Bank USAの両方またはいずれかに、それぞれの鍵で暗号化されて安全に送信されます。Appleはこのデータを復号できません。

申し込み時に提供された所得情報と請求の支払いに使用される銀行口座の情報は、Goldman Sachs Bank USAの鍵で暗号化されてからGoldman Sachs Bank USAに安全に送信されます。銀行口座の情報はキーチェーンに保存されます。Appleはこのデータを復号できません。

AppleウォレットにApple Cardを追加すると、ユーザが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Goldman Sachs Bank USAおよびApple Payments Inc.と共有されることがあります。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でのみ使用されます。

iOS 14.6以降、iPadOS 14.6以降、およびwatchOS 7.5以降では、Apple Cardを所有しているiCloudファミリーの管理者は、iCloudファミリーの13歳以上のメンバーとカードを共有することができます。参加依頼を確認するにはユーザ認証が必要です。Appleウォレットでは、Secure Enclaveの鍵を使用して、オーナーと依頼された人をバインドする署名を計算します。その署名はAppleのサーバで検証されます。

必要に応じて、管理者は参加者の取引限度額を設定できます。また、いつでも参加者のカードをロックして、Appleウォレットの利用を停止することができます。18歳以上の共同オーナーまたは参加者が参加依頼を承諾して入会を申し込んだ場合、AppleウォレットのApple Card申し込みセクションで定められたのと同じ申し込みプロセスを通ります。

Apple Cardの使用状況

物理的なカードはAppleウォレットの「Apple Card」から注文できます。ユーザが物理的なカードを受け取ったあと、カードの2つ折り封筒にあるNFCタグを使ってカードをアクティベートします。このタグはカードごとに一意であり、別のユーザのカードのアクティベートには使用できません。また、Appleウォレットの設定でカードを手動でアクティベートすることもできます。さらに、ユーザがAppleウォレットから物理的なカードをいつでもロックしたりロック解除したりすることもできます。

Apple Cardでの支払いとAppleウォレットパスの詳細

Apple Cardアカウントで行う必要がある支払いは、WebブラウザまたはiOSのAppleウォレットからApple Cashと銀行口座を使って行うことができます。請求の支払いは、Apple Cashと銀行口座による繰り返しまたは特定の日付の1回限りの支払いとしてスケジュールを指定できます。ユーザが支払いを行うと、Apple Cashと同様のアンチリプレイ値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。アンチリプレイ値は、署名を計算するために、支払い設定の詳細と共にSecure Elementに渡されます。その後、署名はApple Payサーバに戻されます。支払いの真正性、整合性、正確性が署名とアンチリプレイ値を使用してApple Payサーバに検証され、注文は処理のためにGoldman Sachs Bank USAに渡されます。

Apple Card番号が証明書の提示によってAppleウォレットに取得されます。Apple Payサーバが証明書を検証し、鍵がSecure Enclaveで生成されたものであることを確認します。サーバは、次にこの鍵を使用して、Appleウォレットに戻す前にApple Card番号を暗号化し、Apple Card番号を要求したiPhoneのみが復号できるようにします。復号後、Apple Card番号はiCloudキーチェーンに保存されます。

Appleウォレットを使ってパスのApple Card番号の詳細を表示するには、Face ID、Touch ID、またはパスコードによるユーザ認証が必要です。この番号はユーザがカード情報セクションで置き換えることができ、その場合、以前の番号は無効になります。

さらに進んだ不正防止機能

iOS 15以降およびiPadOS 15以降では、Apple CardのユーザはAppleウォレットのさらに進んだ不正防止機能を有効にできます。有効にすると、カードのセキュリティコードが数日ごとに更新されます。

Apple Cashのセキュリティ

iOS 11.2以降、iPadOS 13.1以降、およびwatchOS 4.2以降では、Apple CashをiPhone、iPad、またはApple Watchで使用して、ほかのユーザとの間でお金の送金、受領、請求を行うことができます。支払いを受けると、その金額がApple Cashアカウントに加算されます。Apple Cashアカウントには、Appleウォレット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」>「ウォレットとApple Pay」からアクセスできます。

iOS 14、iPadOS 14、およびwatchOS 7では、自らの識別情報をApple Cashで確認済みのiCloudファミリーの管理者は、18歳未満の家族に対してApple Cashを有効にすることができます。管理者は、任意で、これらのユーザの送金機能を家族のみまたは連絡先のみに制限することができます。18歳未満の家族がApple IDアカウントの復旧を実行した場合、ファミリーの管理者はそのユーザに対してApple Cashカードを手動で再度有効にする必要があります。18歳未満の家族がiCloudファミリーのメンバーではなくなると、Apple Cashの残高は管理者のアカウントに自動的に移されます。

ユーザがApple 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ユーザ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。

iMessageでApple Cashを使用する

個人間の送金やApple Cashを使用するには、ユーザがApple 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。ユーザ間の請求と送金は、メッセージアプリ内から、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 Cashの残高が最初に使用されます。必要に応じて、ユーザがAppleウォレットに追加した第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。

店舗、アプリ、Web上でApple Cashを使用する

AppleウォレットのApple CashカードをApple Payで使用して、店舗、アプリ、Web上での支払いも行えます。Apple 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、Appleウォレットのデビットカードまたはプリペイドカードから Apple 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.がユーザの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。ユーザがApple 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。

ユーザがApple Payでの送金、Apple Cashアカウントへの残高追加、銀行口座への送金を行うと、アンチリプレイ値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。アンチリプレイ値は、アプリ内でApple Pay用に返される値と同様の働きをします。アンチリプレイ値は、支払い署名を計算するために、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。署名はApple Payサーバに戻されます。トランザクションの真正性、整合性、正確性が、支払い署名とアンチリプレイ値を使用してApple Payサーバに検証されます。その後送金が実行され、トランザクションの完了がユーザに通知されます。

トランザクションに以下が伴う場合は、

- Apple Cashに残高を追加するためのデビットカード
- Apple Cashの残高不足の場合の不足分の支払い

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。これはアプリ内およびWebサイトでのApple Payの仕組みと同様のものです。

Apple 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（例えばユーザが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。Apple Cashの残高へのアクセスを再度取得する前に、Apple IDアカウントの復旧を実行すると、ユーザに自らの識別情報の確認が求められます。

「iPhoneのタッチ決済」のセキュリティ

加盟店は、iPhoneとパートナー対応のiOSアプリで「iPhoneのタッチ決済」（iOS 15.4以降で利用可能）を使用することで、Apple Payなどの非接触型決済を承認できます。このサービスでは、対応するiPhoneデバイスを所有するユーザが、非接触型決済およびApple PayのNFC対応パスを安全に承認することができます。「iPhoneのタッチ決済」では、非接触型決済を承認するために、店舗が追加でハードウェアを用意する必要はありません。

「iPhoneのタッチ決済」は、支払い者の個人情報を保護できるように設計されています。このサービスは、支払い者が特定される可能性のあるトランザクション情報を収集しません。クレジットカードやデビットカードの番号などの支払い用カード情報（PAN）はSecure Elementで保護され、加盟店のデバイスには表示されません。支払い用カード情報は、加盟店の決済サービスプロバイダ、支払い者、カード発行会社の間に留まります。また、タッチ決済サービスでは、支払い者の名前、住所、電話番号を収集しません。

「iPhoneのタッチ決済」は、公認のセキュリティ機関による外部評価を受けており、「iPhoneのタッチ決済」が利用可能な地域で認められたすべてのペイメントネットワークから使用の承認を受けています。

非接触型決済コンポーネントのセキュリティ

- **Secure Element:** Secure Elementは、非接触型決済カードデータを読み取って保護する決済カーネルをホストしています。
- **NFCコントローラ:** NFCコントローラは、Near Field Communication（NFC）プロトコルに対応し、アプリケーションプロセッサとSecure Element間、およびSecure Elementと非接触型決済カード間の通信をルーティングします。
- **「iPhoneのタッチ決済」のサーバ:** 「iPhoneのタッチ決済」のサーバは、デバイス上の決済カーネルの設定とプロビジョニングを管理します。さらにサーバは、Payment Card Industry Security Standards Council（PCI SSC）のContactless Payments on COTS（CPoC）標準に準拠する方法で「iPhoneのタッチ決済」のセキュリティを監視し、PCI DSSに準拠しています。

タッチ決済がクレジットカード、デビットカード、およびプリペイドカードを読み取る方法

タッチ決済がセキュリティ保証をプロビジョニングする方法

十分なエンタイトルメントのあるアプリで初めて「iPhoneのタッチ決済」を使用すると、「iPhoneのタッチ決済」サーバは、デバイスモデル、iOSバージョン、パスコードが設定されているかなどの資格基準をデバイスが満たしているかを判別します。検証が完了すると、決済承認アプレットが「iPhoneのタッチ決済」サーバからダウンロードされ、関連付けられた決済カーネル構成と共にSecure Elementにインストールされます。この処理は「iPhoneのタッチ決済」サーバとSecure Elementの間で安全に実行されます。Secure Elementはこのデータの整合性と真正性をインストール前に検証します。

タッチ決済がカードを安全に読み取る方法

「iPhoneのタッチ決済」のアプリがProximityReaderフレームワークからカード読み取りを要求すると、iOSが制御するシートが表示され、支払い用カードをタップするようユーザに求めます。アプリでは、タップ画面がアクティブであるときに、機密カードデータのいずれかの部分を漏えいする可能性のあるセンサーを読み取ることはできません。iOSは支払い用カードリーダーを初期化し、Secure Elementの決済カーネルに、カード読み取りを開始するように要求します。

この時点で、Secure ElementはNFCコントローラの制御をリーダーモードで引き受けます。このモードでは、カードデータをNFCコントローラを経由して支払い用カードとSecure Elementの間でのみ交換できます。支払い用カードはこのモード中にのみ読み取れます。

Secure Element上の決済承認アプレットが支払い用カード読み取りを完了すると、カードデータを暗号化して署名します。支払い用カードデータは、決済サービスプロバイダに到達するまでは暗号化されて認証された状態を保ちます。支払い用カードデータの復号は、カード読み取りを要求するアプリが使用する決済サービスプロバイダのみが行うことができます。決済サービスプロバイダは、支払い用カードデータの復号鍵を「iPhoneのタッチ決済」サーバから要求する必要があります。「iPhoneのタッチ決済」サーバは、データの整合性と真正性を検証し、カード読み取りが支払い用カードデータの復号鍵のリクエストから60秒以内に行われたことを確認すると、復号鍵を決済サービスプロバイダに送ります。

このモデルは、店舗向けにこのトランザクションを処理するPSP以外では、支払い用カードデータを復号できないことを保証するのに役立ちます。

PIN入力によるトランザクションの承認

iOS 16.0以降で利用可能なPIN入力では、支払い者が店舗のデバイスにPINを入力して、トランザクションを承認することができます。PIN入力画面は、支払い用カードと交換された情報に基づいて、タップ後すぐにトリガすることができます。また、決済サービスプロバイダが1回のトランザクションでのみ有効な署名済みトークンを提供することで、PIN画面をトリガすることもできます。

PIN入力のメカニズムは、公認のセキュリティ機関による外部評価を受けており、PIN入力が利用可能な地域で認められたすべてのペイメントネットワークから使用の承認を受けています。PIN入力画面はスクリーンショットや画面ミラーリングから保護されており、PIN入力画面がアクティブな間は、いかなるアプリも、PIN値のいずれかの部分を漏えいする可能性のあるセンサーを読み取ることはできません。

入力されたPINの数字は、Secure Elementによって安全に取得されます。これらのPINの数字を使用して、Secure Elementは決済業界標準に準拠した暗号化PINブロックを作成します。Appleは、暗号化PINブロックをPCI PIN準拠のバックエンドからPSPに安全に提供し、さらなる処理に回します。

PIN値は:

- 店舗のデバイスでは決して利用できません
- いかなる場合もAppleが復号することはありません
- Appleが保存することは決してありません

Appleウォレットを使用する

Appleウォレットを使用したアクセス

対応するiPhoneとApple WatchデバイスのAppleウォレットでは、さまざまなタイプの鍵を保存できます。ドアの前に到着すると、(その鍵がエクスプレスモードに対応していて、エクスプレスモードがオンの場合は)適切な鍵が自動的に表示されるので、タップするだけで近距離無線通信(NFC)を使って中に入ることができます。

ユーザに便利なこと

エクスプレスモード

Appleウォレットに鍵を追加すると、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鍵は、Face ID、Touch ID、パスコードによる認証、またはApple Watchのサイドボタンのダブルクリックなしで、受け入れ側端末とやりとりします。この機能を無効にするには、Appleウォレットで鍵を示すカードの前面の「その他」ボタンをタップしてエクスプレスモードをオフにします。エクスプレスモードをオンに戻すには、Face ID、Touch IDまたはパスコードを使用する必要があります。

キーの共有

iOS 16以降では、特定のキーのタイプでキーの共有を利用できます。

ユーザは、キー(家のキーや車のキーなど)の所有者のiPhoneから参加依頼されたキー受取人のiPhoneにセキュリティとプライバシーを適用して、そのキーへのアクセスを共有することができます。 キーは、Appleウォレットのキーの共有アイコンをタップすることで共有され、共有シートに表示される方法を使用して共有することができます。また、キー所有者は、共有キーごとのアクセスレベルと有効期間を選択することもできます。キー所有者は共有したすべてのキーを表示でき、最初のキー受取人がキーを別のユーザに再度共有している場合を含み、共有キーのアクセスを取り消すことができます。

キーの共有の参加依頼は、メールボックス内の専用サーバによって匿名化および保護された状態で保存され、AES 128または256暗号鍵で保護されます。暗号鍵はサーバや意図したキー受取人以外の誰とも共有されることはなく、参加依頼を復号できるのはキー受取人のみです。メールボックスの作成時に、キー所有者のiPhoneが、サーバによってそのメールボックスにのみバインドされているデバイス要求を提供します。キー受取人のiPhoneが最初にこのメールボックスにアクセスすると、キー受取人にデバイス要求が提示されます。キー所有者と、有効なデバイス要求が提示されるキー受取人のiPhoneデバイスのみが、そのメールボックスにアクセスできます。各iPhoneデバイス要求には、RFC4122の通り、一意のUUID値が含まれています。

キー所有者は、追加のセキュリティ対策として、キー受取人のiPhoneで必要な6桁のランダムに生成されたアクティベーションコードをオンにすることができます。コードの再試行回数は、キー所有者またはパートナーサーバのいずれかによって適用され、検証されます。このアクティベーションコードはキー所有者がキー受取人に伝える必要があり、キー受取人はキー所有者またはパートナーサーバによって検証を求められたときに、そのコードを提示する必要があります。

参加依頼がキー受取人によって使用されると、受信側のiPhoneによってサーバからすぐにワイプされます。また、キーの共有の参加依頼が含まれているメールボックスは、有効期間が制限されています。この有効期間はメールボックスの作成時に設定され、サーバによって適用されます。期限切れの参加依頼は、サーバによって自動的に消去されます。

元の製造元によっては、キーがApple以外のデバイスと共有されることもあります。ただし、キーの共有の保護の方法は、Appleの方法とは異なる場合があります。

プライバシーおよびセキュリティ

Appleウォレットのアクセス鍵では、iPhoneとApple Watchに組み込まれたプライバシーとセキュリティが最大限に活用されます。ある人がいつどこでAppleウォレットの鍵を使用したかがAppleと共有されたりAppleのサーバに保存されたりすることはなく、資格情報は対応デバイスのSecure Elementに安全に保存されます。Secure Elementは、鍵を安全に管理するために特別に設計されたアプレットをホストすることで、鍵を抽出したり漏えいしたりできないことを保証します。

鍵のプロビジョニング前に、ユーザが対応するiPhoneでiCloudアカウントにサインインし、iCloudアカウントで2ファクタ認証をオンにする必要があります。ただし、学生証の場合は2ファクタ認証をオンにする必要はありません。

ユーザがプロビジョニングプロセスを開始すると、リンクやプロビジョニングなど、クレジットカードやデビットカードのプロビジョニングと同様の手順が行われます。トランザクションの実行中、リーダーは確立されたセキュアチャネルを使用して、Near -Field -Communication（NFC）コントローラ経由でSecure Elementと通信します。

1つの鍵でプロビジョニングできるデバイスの数（iPhoneとApple Watchを含む）は、各パートナーによって定められ、パートナーごとに異なります。このアプローチによって、各パートナーがデバイスタイプごとにプロビジョニングできる鍵の最大数をそれぞれのニーズに合わせて制御することができます。この目的のために、Appleはパートナーにデバイスタイプおよび匿名化されたデバイスの識別子を提供します。プライバシーとセキュリティ上の理由により、識別子はパートナーごとに異なります。

パートナーは、匿名化された、パートナーごとに一意のユーザ識別情報も受信します。このユーザ識別情報を使用して、最初のプロビジョニング中にユーザのiCloudアカウントに鍵を安全にバインドすることができます。この対策により、パートナーと作成したユーザアカウントが侵害された場合に（アカウント乗っ取り攻撃のシナリオなど）、キーが別のユーザによってプロビジョニングされないように保護されます。

鍵は以下の方法で無効にしたり削除したりできます:

- 「探す」でデバイスをリモートで消去する
- 「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受信する
- 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
- Appleウォレットからすべてのカードを削除する
- 発行会社のアプリでカードを削除する

iOS 15.4以降では、Face IDを搭載したiPhoneのサイドボタンをダブルクリックする、あるいはTouch IDを搭載したiPhoneのホームボタンをダブルクリックしても、デバイスから認証されるまでパスやアクセス鍵の詳細は表示されません。Appleウォレットにホテル予約の詳細などのパスの具体的な情報を表示するには、Face ID、Touch ID、またはパスコード認証が必要です。

アクセス鍵のタイプ

Appleウォレットのアクセスには、宿泊施設、社員証、学生証、家の鍵、車の鍵など、さまざまなタイプがあります。

宿泊施設

Appleウォレット内のホテルルームの鍵では、チェックインからチェックアウトまで簡単に非接触で行うことができ、従来のプラスチック製のホテルキーカードを上回るプライバシーおよびセキュリティ上の利点をゲストに提供できます。対応しているホテルのゲストは、互換性のあるiPhoneおよびApple Watch Series 4以降のAppleウォレット内にある部屋の鍵を使って、タップしてドアを解錠できます。

Appleウォレットの機能は、お客様の手間を減らすように特別に設計されています:

- ホテルのアプリから到着前にプロビジョニングする。滞在前にパスをAppleウォレットに追加する
- チェックインパスのタイル。Appleウォレットからチェックインと部屋割りを開始する
- プロビジョニング後の鍵アップデート。現在の滞在を延長または修正する
- Appleウォレット内の1つのパスで、複数のルーム鍵に対応
- Appleウォレット内で期限切れの鍵を自動アーカイブ

Disney MagicMobile Pass

ユーザはiPhoneまたはApple WatchのAppleウォレットにDisney MagicMobile Passを追加して、加入しているディズニーテーマパークに入園することができます。MagicMobile Passはパークへの入園に使用でき、パーク内の対応するその他の読み取り機でも使用できます。

Disney MagicMobile Passを追加するには、iCloudアカウントで2ファクタ認証が有効になっていることに加えて、ユーザが有効なMy Disney Experienceアカウントに関連付けられた加入しているテーマパークのチケットまたは予約を持っている必要があります。ユーザは、iPhoneのMy Disney Experienceアプリから、1つまたは複数のパスを選択してAppleウォレットに追加することができます。Apple Watchがペアリングしてあれば、選択したパスがユーザのiPhoneとペアリングされたApple Watchの両方に自動的にプロビジョニングされます。iPhoneおよびApple Watchデバイスの両方に追加されたパスには、エクスプレスモードがデフォルトでオンになります。簡単に使用できるように、エクスプレスモードがオンになっている場合は、現時点でデバイス上のすべてのMagicMobileパスでオンになります。

1台のデバイスに複数のパスを追加して、ユーザが自分のグループのすべてのメンバーのパスを管理できるようにすることができます。また、ユーザは、My Disney Experienceアプリを使用してほかのユーザとパスを共有することも選択できます。この方法で、受信者が共有パスを自分のデバイスのAppleウォレットに追加することができます。

社員証

対応するパートナーの社員証をiPhoneおよびApple WatchのAppleウォレットに追加することで、世界中の従業員が職場に非接触で入ることができます。社員証を追加するには、雇用主から提供されたアプリにサインインするのに使用するアカウントで、従業員が多要素認証を有効にする必要があります。

社員証では、Appleのアクセス機能を利用して次のことができます:

- パートナーのアプリをインストールする必要がないプッシュプロビジョニングによって、ペアリングされたApple Watchに社員証を自動的に追加する
- エクスプレスモードを利用してシームレスにオフィス設備にアクセスする
- iPhoneのバッテリーが切れたあとでも職場にアクセスする

学生証

iOS 12以降では、対応している学校の学生や教職員が、対応するiPhoneおよびApple WatchのAppleウォレットに学生証を追加して、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、学生証の発行会社または学校が提供するアプリを使用してAppleウォレットに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、カード発行会社のアプリ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で説明している内容と同じです。また、発行に使用するアプリは、学生証情報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、ユーザのiPhoneとペアリングされたApple Watchで同時に設定できます。

集合住宅

対応するパートナー施設のテナントとスタッフは、Appleウォレットのホームキーを使って建物、ユニット、共用部分にアクセスできます。ホームキーはパートナーが提供するアプリからプロビジョニングできます。手間のかからないプロビジョニングに対応したパートナーでは、建物の管理者がテナントの希望に合わせた連絡方法（メールやSMSなど）でプロビジョニング開始用のリンクをテナントに送信し、リンクをクリックすればキーを使えるようにできます。App Clipでも安全でシームレスな体験が提供されます。パートナーのアプリをインストールせずにキーをプロビジョニングできます。詳しくは、Appleサポートの記事「iPhoneでApp Clipを使用する」を参照してください。

集合住宅のホームキーはエクスプレスモードで使用することもでき、友達や家族と安全に共有することができます。詳しくは、キーの共有を参照してください。

ホームキー

Appleウォレットのホームキーを使用すると、iPhoneまたはApple Watchをタップするだけで、対応しているNFCドアロックを解錠できます。ホームキーの設定と使用について詳しくは、Appleサポートの記事「iPhoneのホームキーでドアを解錠する」を参照してください。

1人がホームキーを設定すると、その世帯の居住者全員も自動的にホームキーを受け取ります。ホームキーをさらに共有したり、共有ホームのメンバーを削除したりする場合は、ホームの所有者がホームアプリを使って参加依頼とメンバーを管理できます。ホームキーのあるホームへの参加依頼をユーザが承諾すると、そのユーザのデバイスのAppleウォレットにホームキーのプロビジョニングが開始されます。ユーザがホームへの参加をやめるか、ホームの所有者がアクセスを取り消すと、Appleウォレットからもホームキーが削除されます。

車のキー

Appleウォレットにデジタルに車のキーを保存する機能は、対応したiPhoneデバイスおよびペアリングされたApple Watchデバイスでネイティブに利用できます。車のキーは（Appleが自動車メーカーの代理として作成した）Appleウォレット内のパスとして表現され、Apple Payカードのライフサイクル全体（iCloud紛失モード、リモートワイプ、ローカルパス削除、すべてのコンテンツと設定を消去）に対応しています。標準的なApple Payカードと同様、共有の車のキーは、所有者のiPhone、Apple Watch、車両のヒューマンマシンインターフェイス（HMI）から削除できます。

車のキーは例えば、車両をロック解除/ロックする、トランクを開閉する、アラームをオン/オフする、エンジンをかける、車両をドライブモードに設定するといったことに使えます。「標準トランザクション」は相互認証を提供し、エンジン始動には必須です。解錠/施錠のトランザクションでは、パフォーマンス上の理由で必要な場合は「高速トランザクション」を使用する場合があります。

キーの作成は、所有している対応する車両にiPhoneを接続（またはペアリング）することで行います。すべてのキーはSecure Element内で楕円曲線（NIST P-256）オンボード鍵生成（ECC-OBKG）に基づいて作成され、秘密鍵がSecure Elementを離れることはありません。デバイスと車両の間の通信にはNFCまたはBluetooth® LEと超広帯域無線（UWB）の組み合わせが使用されます。キーの管理にはAppleから自動車製造元サーバへのAPIと相互認証済みTLSが使用されます。キーがiPhoneとペアリングされると、そのiPhoneとペアリングされたApple Watchでもキーを受け取ることができます。車両またはデバイスのいずれかでキーが削除されると、キーは復元できなくなります。紛失したデバイスや盗まれたデバイスのキーは一時停止してから再開できますが、新しいデバイスに再度プロビジョニングするには、新しくペアリングしたり共有したりする必要があります。

車のキーはエクスプレスモードで使用することもでき、友達や家族と安全に共有することができます。詳しくは、キーの共有を参照してください。車のデジタルキーのセキュリティとプライバシーについて詳しくは、iOSでの車のキーのセキュリティを参照してください。

スクーターのキー

iOS 17以降、および特定の国または地域と対応するパートナーでは、ユーザは以下の目的のために、スクーターのキーをパートナーアプリから対応するiPhoneとペアリングされたApple WatchのAppleウォレットに直接プロビジョニングすることができます:

- タップしてスクーターをロックする/ロック解除する
- タップしてスクーターのトランクをロックする/ロック解除する(使用可能な場合)

Secure Elementの専用アプレットは、スクーターのキーに関連付けられた暗号化資格情報を安全に処理し、スクーターとの安全なトランザクションを許可します。

パスの裏側では、ユーザは、車両識別番号(VIN)の最後の4桁とその免許証やナンバープレートなど、スクーターに関するその他の情報にアクセスできます。そのような情報は個人情報と見なされる場合があり、生体認証やデバイスパスコードを使用する場合のみアクセスできます。

スクーターのキーはエクスプレスモードで使用することもでき、友達や家族と安全に共有することができます。詳しくは、キーの共有を参照してください。

iOSでの車のキーのセキュリティ

デベロッパは、対応しているiPhoneとペアリングされているApple Watchで車両にアクセスするための安全なキーレスの方法をサポートできます。

オーナーのペアリング

オーナーが自動車メーカーまたは車両のメニューから受け取ったメールのリンクを使用して自動車メーカーのアプリでペアリングプロセスを始めるには、自分がその車両のオーナーであることを証明する必要があります(方法は自動車メーカーによって異なります)。いかなる場合でも、オーナーは秘密の1回限りのペアリングパスワードをiPhoneに提示する必要があります。このパスワードは、SPAKE2+プロトコルとNIST P-256曲線を使用して安全なペアリングチャネルを生成するのに使用されます。アプリまたはメールのリンクを使用するときは、パスワードは自動的にiPhoneに転送されます。車両からペアリングを始めるときは手動で入力する必要があります。

キーの共有

オーナーのペアリングされたiPhoneは、iMessageとApple Identity Service(IDS)を使用してデバイス固有の招待を送ることで、資格のある家族や友達のiPhoneデバイスとキーを共有できます(ペアリングされたApple Watchデバイスとも共有できます)。すべての共有コマンドはエンドツーエンドの暗号化されたIDS機能を使用して交換されます。オーナーのペアリングされたiPhoneは、招待の転送から保護するために、共有プロセス中にIDSチャネルが変わらないようにします。

招待を承諾すると、家族や友達のiPhoneはデジタルキーを作成し、キーが真正のAppleデバイスで作成されたことを検証するために、キー作成証明書チェーンをオーナーのペアリングされたiPhoneに送り返します。オーナーのペアリングされたiPhoneは、家族や友達のiPhoneのECC公開鍵に署名し、その署名を家族や友達のiPhoneに送り返します。オーナーデバイスでの署名操作には、Face ID、Touch IDの用途で説明されているユーザ認証(Face ID、Touch ID、またはパスコード入力)と確実なユーザによる意思表示が必要です。認証は、招待を送るときに要求され、友達のデバイスが署名リクエストを送り返したときに消費用セキュアエレメントに保存されます。キーのエンタイトルメントは、車両OEMサーバによってオンラインで車両に提供されるか、車両の共有キーを初めて使用しているときに車両に提供されます。

キーの削除

キーホルダーデバイスにあるキーは、オーナーデバイスや車両から削除できます。キーホルダーiPhoneでの削除はすぐに実行されます(キーホルダーでキーが使用されている場合でも)。そのため、削除の前に強い警告が表示されます。車両からのキーの削除は、いつでも可能な場合と、車両がオンラインのときにのみ可能な場合があります。

どちらの場合でも、キーホルダーデバイスまたは車両での削除は、自動車メーカー側のキーインベントリサーバ(KIS)に報告されます。サーバは保険の目的で発行済みの車のキーを登録します。

オーナーはオーナーパスの背面から削除を要求できます。この要求は、車両でのキー削除のために最初に自動車メーカーに送信されます。車両からキーを削除するための条件は、自動車メーカーによって定義されています。車両でキーが削除された場合のみ、自動車メーカーからキーホルダーデバイスにリモートの終了リクエストが送信されます。

車両でキーが終了すると、デジタルの車のキーを管理するアプレットにより署名済み終了証明が暗号化されて作成されます。この証明は、自動車メーカーが削除の証明として使用し、KISからキーを削除するために使用します。

NFC標準トランザクション

NFC鍵を使用している車両では、リーダーとiPhone間のセキュアチャネルは、リーダーおよびiPhone側で一時的な鍵ペアを生成することによって開始されます。鍵共有法を使用することで、共有シークレットを両方の側で導出して、Diffie-Hellman、鍵導出関数、およびペアリング時に確立された長期鍵からの署名を使用した共有対称鍵の生成に使用できます。

車両側で生成される一時公開鍵は、リーダーの長期秘密鍵で署名されます。これにより、iPhone側でリーダーが認証されます。iPhone側から見れば、このプロトコルはプライバシーに関わるデータが通信を傍受する敵に暴露されないように設計されています。

最後に、iPhoneは確立されたセキュアチャネルを使用して、その公開鍵識別子を、リーダーのデータ導出チャレンジといくつかのアプリ固有追加データで計算された署名と共に暗号化します。リーダー側は、iPhone署名を検証することにより、デバイスを認証できます。

高速トランザクション

iPhoneは、標準トランザクション中に以前に共有されたシークレットに基づいて暗号文を生成します。この暗号文により、車両はパフォーマンスの影響を受けるシナリオでデバイスを素早く認証できます。必要に応じて、以前に標準トランザクション時に共有されたシークレットと新しい一時鍵のペアからセッション鍵を導出することで、車両とデバイス間にセキュアチャネルが確立されます。車両がセキュアチャネルを確立できれば、車両はiPhoneから認証されたことになります。

BLE/UWB標準トランザクション

UWB鍵を使用している車両では、車両とiPhoneの間でBluetooth LEセッションが確立されます。NFCトランザクションと同様に、共有シークレットが両方の側で導出され、安全なセッションの確立に使用されます。このセッションは、UWB測距秘密鍵(URSK)を導出して合意するために使用されます。URSKは、ユーザのデバイスと車両のUWB無線に対して、ユーザのデバイスが車両の近くまたは車両内のどこにあるかを正確に測定するために提供されます。車両はデバイスの位置を使用して、車両のロック解除または起動を許可するかどうかを判断します。URSKにはあらかじめTTLが定義されています。TTLの期限が切れたときに測距が中断するのを回避するために、安全な測距はアクティブでないけれどもBLEが接続されている間に、デバイスSEと車両HSM/SEでURSKをあらかじめ導出しておくことができます。これにより、標準トランザクションが時間の限られた状況で新しいURSKを導出する必要がなくなります。あらかじめ導出されたURSKを車とデバイスのUWB無線に素早く転送することで、UWB測距の中断を回避できます。

プライバシー

自動車メーカーのキーインベントリサーバ(KIS)には、デバイスID、SEID、またはApple IDは保存されません。保存されるのは更新可能識別子(インスタンスCA識別子)のみです。この識別子はデバイス内またはサーバ側の個人データに紐づけられておらず、ユーザが「すべてのコンテンツと設定を消去」を使用してそのデバイスを完全にワイプすると削除されます。

Appleウォレットに交通系ICカードや電子マネーカードを追加する

世界の多くの市場で、対応するiPhoneおよびApple WatchモデルのAppleウォレットに、対応する交通系ICカードや電子マネーカードを追加できます。これは、運営会社に応じて、物理的なカードからAppleウォレットのデジタルデータに残高や定期券（またはその両方）を転送するか、Appleウォレットまたは交通系ICカードや電子マネーカードの発行会社が提供するアプリで新しいカードを作成して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Appleウォレットに追加すると、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。一部の交通系ICカードは支払いにも使用できます。

交通系ICカードや電子マネーカードの仕組み

追加した交通系ICカードや電子マネーカードはユーザの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Appleウォレットに追加すると、Appleまたは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。交通系ICカードや電子マネーカードおよび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Appleウォレットに残高が転送される処理では、ユーザにカード固有の情報の入力が求められます。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。iPhoneからApple Watchにカードを転送するときは、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、Appleウォレット経由で、または交通系ICカードや電子マネーカードの発行会社のアプリから、クレジットカード、デビ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、アプリ内でカードで支払うを参照してください。カードの発行会社のアプリ内で行われるカードのプロビジョニング方法については、カード発行会社のアプリ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を参照してください。

物理的なカードからのプロビジョニングがサポートされている場合、交通系ICカードや電子マネーカードの発行会社は、物理的なカードの認証と、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。データの検証が完了すると、システムはSecure Element用のデバイスアカウント番号を作成し、新しく追加されたパスに転送された残高を追加してAppleウォレットで有効にすることができます。一部のカードでは、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、カードの残高がデバイスに保存されている場合、プロビジョニングの終了後に残高が暗号化され、Secure Element内の指定されたアプレットに保存されます。カードの運営会社は、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。

交通系ICカードの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、Face ID、Touch 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「ウォレットとApple Pay」設定で「エクスプレスカード」を無効にすることで、Face ID、Touch ID、またはパスコードによる認証の要求をオンにすることができます。電子マネーカードはエクスプレスモードに対応していません。

Apple Payのほかのカードと同様に、電子マネーカードでは、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。

- 「探す」でデバイスをリモートで消去する
- 「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入力する
- 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
- Appleウォレットからすべてのカードを削除する
- 発行会社のアプリでカードを削除する

Apple Payサーバからカードの運営会社に、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。ユーザがオンラインのデバイスから交通系ICカードや電子マネー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。デバイスがオフラインになっているか、電源がオフになっているか、使用できない場合は、残高を回収できません。

ファミリーメンバーのApple Watchに交通系ICカードや電子マネーカードを追加する

iOS 15以降、およびwatchOS 8以降では、iCloudファミリーの管理者がiPhoneのApple Watchアプリを経由して、交通系ICカードや電子マネーカードをファミリーメンバーのApple Watchデバイスに追加することができます。これらのカードの1枚をファミリーメンバーのApple Watchにプロビジョニングするときには、Apple Watchが近くにあり、Wi-FiまたはBluetoothで管理者のiPhoneに接続されている必要があります。そのためには、ファミリーメンバーがApple IDの2ファクタ認証を有効にしておく必要があります。

ファミリーメンバーは、Apple WatchのiMessageを使って、交通系ICカードや電子マネーカードに残高を追加するリクエストを送ることができます。iMessageのセキュリティの概要で説明されている通り、メッセージの内容はエンドツーエンドの暗号化によって保護されます。ファミリーメンバーのApple Watch上のカードに残高を追加する操作は、Wi-Fi接続またはモバイルデータ通信接続によってリモートで行うことができます。近くにいる必要はありません。

注記: 国や地域によっては、この機能を利用できない場合があります。

クレジットカードとデビットカード

一部の都市では、改札機は交通機関利用の支払いにEMV(スマート)カードを受け入れます。ユーザがそれらの改札機にEMVクレジットカードまたはデビットカードを提示する場合、「店舗でクレジットカードおよびデビットカードを使用して支払う」のと同様に、ユーザの認証が必要です。

iOS 12.3以降では、Appleウォレットに追加済みの一部のEMVクレジット/デビットカードをエクスプレスカードとして有効にできます。エクスプレスカードでは、ユーザはFace ID、Touch ID、またはパスコードを要求されることなく、対応する交通機関の料金を支払うことができます。ユーザがEMVクレジットカードまたはEMVデビットカードをプロビジョニングすると、Appleウォレットにプロビジョニング済みの最初のカードがエクスプレスカードとして有効になります。ユーザは、Appleウォレットでカードの前面に表示される「詳細」ボタンをタップし、「エクスプレスカード設定」を「なし」に設定することで、そのカードをエクスプレスカードとして無効にすることができます。また、ユーザはAppleウォレットで別のクレジットカードまたはデビットカードをエクスプレスカードとして選択することもできます。エクスプレスカードとして再度有効にするか、別のカードを選択するときは、Face ID、Touch ID、またはパスコードが必要になります。

Apple CardとApple Cashはエクスプレスカードとして設定できます。

Appleウォレットでの本人確認書類

Appleウォレットでの本人確認書類

iOS 15.4以降が搭載されたiPhone 8以降、およびwatchOS 8.4以降が搭載されたApple Watch Series 4以降では、州発行の本人確認書類や運転免許証をAppleウォレットに追加して、iPhoneまたはApple Watchをタップすれば対応する場所でシームレスかつ安全にそれらの証明書を提示することができます。

注記: この機能は対応する米国の州でのみ利用できます。

Appleウォレットの本人確認書類は、ユーザのデバイスのハードウェアとソフトウェアに組み込まれたセキュリティ機能を使用して、ユーザの識別情報を保護し、個人情報を安全に保つのに役立ちます。

Appleウォレットに運転免許証や州発行の本人確認書類を追加する

iPhoneで、Appleウォレットの画面上部にある「追加」ボタン(+)をタップするだけで、免許証や本人確認書類の追加を始めることができます。設定時にApple Watchがペアリングしてあれば、運転免許証や本人確認書類をApple WatchのAppleウォレットにも追加するように求められます。

まず、iPhoneで物理的な運転免許証や州発行の本人確認書類の表と裏をスキャンするように求められます。提出した画像が州の発行機関に確実に承認されるよう、画像の品質と種類がiPhoneによって評価されます。これらの本人確認書類の画像はデバイス上にある州の発行機関の鍵で暗号化され、州の発行機関に送信されます。

次に、一連の顔や頭の動きを行うように求められます。これらの動きはユーザのデバイスとAppleにより評価され、誰かが写真、ビデオ、マスクを使って他人の本人確認書類をAppleウォレットに追加しようとするリスクを減らすのに役立てられます。これらの動きを分析した結果は州の発行機関に送信されますが、動き自体のビデオは送信されません。

Appleウォレットに本人確認書類を追加しようとしている人がその書類の所有者と同一人物であることを確認するため、セルフィーを撮影するよう求められます。ユーザの写真が州の発行機関に提出される前に、Appleのサーバとユーザのデバイスではその写真と一連の顔や頭の動きを行った人の外観が比較され、提出される写真が本人確認書類の写真と同じ外観を持つ生身の人間のものであることを確認するのに役立てられます。比較の完了後、本人確認書類用に登録されている画像と照合するために、写真はデバイス上で暗号化されて州の発行機関に送信されます。

最後に、Face IDまたはTouch IDによる認証を行うように求められます。ユーザのデバイスはこの照合された単一のFace IDまたはTouch IDの生体認証を州発行の本人確認書類に結びつけ、その本人確認書類をこのiPhoneに追加した人のみが提示できるようにします。登録されているその他の生体認証情報は、本人確認書類の提示を承認するのに使用することはできません。これは厳密にデバイスでのみ実行され、州の発行機関には送信されません。

州の発行機関は、デジタル本人確認書類を設定するのに必要な情報を受け取ります。これには、ユーザの本人確認書類の表と裏の画像、PDF417バーコードから読み取ったデータに加え、本人確認書類の確認プロセスでユーザが撮影したセルフィーも含まれます。州の発行機関はさらに、不正を防止するのに使用される、ユーザのデバイス使用パターンに基づいた1桁の値、設定データ、および個人のApple IDに関する情報を受け取ります。最終的には、本人確認書類のAppleウォレットへの追加を承認するか拒否するかは州の発行機関が決定します。

州の発行機関によって州発行の本人確認書類または運転免許証のAppleウォレットへの追加が承認されると、iPhoneのSecure Elementで、ユーザの本人確認書類をその特定のデバイスに固定する鍵ペアが生成されます。Apple Watchに追加した場合は、Apple WatchのSecure Elementで鍵ペアが生成されます。

本人確認書類がiPhoneに追加されると、Appleウォレット内のユーザの本人確認書類に反映された情報は、Secure Elementで保護された暗号化フォーマットで保存されます。

Appleウォレット内の運転免許証や州発行の本人確認書類をリーダーで使用する

Appleウォレット内の本人確認書類を使用するには、iPhoneが情報をリーダーに提示する前に、Appleウォレット内の本人確認書類と関連付けられたデバイスをユーザがFace IDまたはTouch IDで認証する必要があります。

Apple WatchのAppleウォレット内にある本人確認書類を使用するには、ユーザがApple Watchを装着するたびに、関連付けられたFace IDの容姿やTouch IDの指紋でiPhoneをロック解除する必要があります。そのあとは、Apple Watchを外すまで、認証なしでAppleウォレット内の本人確認書類を使うことができます。この機能では、watchOSのシステムのセキュリティで詳述されている基盤となる自動ロック解除機能を活用しています。

iPhoneまたはApple Watchをリーダーにかざすか、アプリ内で本人確認書類を共有すると、どの特定の情報が誰によって要求されているか、および情報を保存するかどうかを示すプロンプトがデバイスに表示されます。関連付けられたFace IDまたはTouch IDで承認すると、要求された識別情報がデバイスから渡されます。

重要: 本人確認書類を提示する際に、デバイスのロックを解除したり、デバイスを見せたり手渡したりする必要はありません。

Face IDまたはTouch IDを有効にする代わりに、音声コントロール、スイッチコントロール、またはAssistiveTouchなどのアクセシビリティ機能を使用している場合は、パスコードを使って情報のアクセスと提示を行うことができます。

識別情報データのリーダーへの送信は、ISO/IEC 18013-5規格に従っています。この規格は、セキュリティリスクを検知、抑止、軽減できる複数のセキュリティメカニズムを規定しています。これらのメカニズムは、識別情報データの整合性と偽造防止、デバイスのバインディング、インフォームドコンセント、無線リンクでのユーザデータの機密性で構成されます。

Appleウォレット内の運転免許証や州発行の本人確認書類をiOSアプリで使用する

ユーザは、Appleウォレット内の運転免許証や州発行の本人確認書類の情報をiOSアプリと共有することもできます。ユーザが本人確認書類をアプリと共有すると、ウォレットはアプリのデベロッパが登録した暗号化証明書を取得および検証します。

この証明書は、ユーザが共有することに同意した情報を暗号化するのに使用されます。この情報はウォレットによってHPKEを使用して暗号化され、Appleが利用できるようになることはありません。ウォレットは定期的にAppleサーバにクエリを実行し、本人確認書類がまだ有効であるかを検証します。しばらくチェックが行われていない場合は、ユーザが本人確認書類をアプリと共有した際にチェックが行われる場合があります。

Appleウォレットでの本人確認書類のセキュリティ

以下の機能は、Appleウォレットで使用する本人確認書類のセキュリティを向上させることができます。

識別情報データの整合性と偽造防止

Appleウォレットの本人確認書類では、発行機関が提供した署名を使用して、ISO/IEC 18013-5に準拠したリーダーによるAppleウォレットのユーザの本人確認書類の検証を許可します。さらに、ウォレットの本人確認書類にあるすべてのデータ要素は、個別に偽造から保護されています。これによって、リーダーがAppleウォレット内の本人確認書類に存在するデータ要素の特定のサブセットを要求し、Appleウォレット内の本人確認書類がその同じサブセットを返すことができます。こうしたことの結果、要求されたデータを共有し、ユーザのプライバシーを最大化できます。

デバイスのバインディング

Appleウォレット認証の本人確認書類は、デバイス署名を使用して、本人確認書類の複製や識別情報提示のリプレイから保護します。Appleウォレットが本人確認書類認証の秘密鍵をiPhoneデバイスのSecure Elementに保存することで、本人確認書類は州の発行機関が本人確認書類を作成したのと同じデバイスにバインドされます。

インフォームドコンセント

Appleウォレットの本人確認書類は、ISO/IEC 18013-5規格で定められたプロトコルを使用して、リーダーを識別するために認証を使用する場合があります。提示中、Appleウォレットに信頼された固有の証明書がリーダーにある場合は、やりとりしている相手が意図した相手である保証をユーザに与えるためにアイコンが表示されます。

無線リンク上のユーザデータの機密性

セッションの暗号化によって、Appleウォレット内の本人確認書類とリーダーの間で交換されるすべての個人を特定できる情報（PII）が暗号化されることが保証されます。暗号化はアプリケーションレイヤーで実行されます。そのため、セッション暗号化のセキュリティは、送信レイヤー（NFC、Bluetooth、Wi-Fiなど）で提供されるセキュリティには依存しません。

Appleウォレットの本人確認書類は、ユーザの情報を非公開に保つのに役立つ

Appleウォレットの本人確認書類は、ISO/IEC 18013-5に示された「デバイス検索」プロセスに従っています。デバイス検索によって提示中にサーバを呼び出す必要がなくなり、ユーザがAppleおよび発行機関の追跡から保護されます。

ID確認のセキュリティ

iOS 17以降では、米国の企業や組織は、外部ハードウェアを必要とせずに、iPhoneを使用してシームレスで安全に、対面でISO 18013-5準拠のモバイルIDを読み取ることができます。ID確認は、確認のユースケースに応じて2つの異なる方法で使用できます:

- **ID確認の表示のみ:** これにより、iOSユーザインターフェイスを使用して、視覚的な確認のみが必要なユースケースで「名前」、「年齢」、「身分証明写真」、および「**N**歳以上」のデータを表示できるようになります。このサービスは、提示者が特定される可能性のある**個人を特定できる情報**(PII)の収集を許可しません。
- **ID確認データ転送:** これにより、法的な確認要件を満たすために、アプリで誕生日や住所などの追加のデータ要素を要求できるようになります。ID確認データ転送APIへのアクセスはエンタイトルメントで管理され、アプリはデータの利用方法に関する要件に準拠する必要があります。例えば、アプリは、本人データを要求するために法的な要件を示す必要があります。また、要求した本人データの処理、保存、またはその他の使用について詳細に規定したプライバシーポリシーを維持することも要求されます。

モバイルIDの読み取り

ID確認は、ISO/IEC 18013-5規格で定められたプロトコルに従います。ID確認APIを使用するアプリがモバイルIDを読み取るよう要求すると、iOSによって制御されるシートが表示され、モバイルIDの持ち主にデバイスをリーダーに近づけるよう求めます。その最初のNFCの関与(ISO/IEC 18013-5規格によって定義されているように、QRコードを使用して、NFCの代わりにBluetoothハンドオーバープロセスを開始できます)により、両方のデバイス間に安全なBluetooth® Low Energy(BLE)接続が確立されます。その時点で、モバイルIDの持ち主は、要求されている情報を自分のデバイスで確認することができます。モバイルIDの持ち主が同意すると、要求された本人データが読み取り側デバイスに転送されます。ID確認データ転送APIを使用するアプリは処理のために応答データを受信し、ID確認の表示のみAPIを使用するアプリは、iOSによって直接表示されるデータを表示します。

ISO/IEC 18013-5規格は、セキュリティリスクを検知、抑止、軽減する複数のセキュリティメカニズムを規定しています。その中でID確認は、発行機関の署名とデバイス署名の検証の両方を実行します。さらに、ID確認は、ISO/IEC 18013-5規格で定められたプロトコルを使用したリーダー認証に対応しています。アプリは、リーダーの証明書を使用してIDの持ち主がやりとりしている相手が意図した相手であるという保証を与えるために、アイコンと名前を表示することを選択できます。

発行機関とデバイスの検証

偽造からの保護として、ID確認は、モバイルIDの信頼できる発行機関によるモバイルセキュリティオブジェクトの署名を検証します。ID確認データ転送は、必要に応じて、iOSではなくアプリで独自の署名の検証を実施できるようにするAPIも提供します。企業や組織にモバイルIDがデバイス間でコピーされていないという保証を与えるため、ID確認はセッションデータで署名を検証します。

リーダー認証

提示の時点で、ID確認リーダーのリクエストが、Appleルート認証局(CA)までチェーンするリーダー認証証明書に関連付けられた秘密鍵によって署名されます。これには、企業がデータを保存する予定の場合に持ち主に示す、関連のx509のカスタム機能拡張が含まれています。アプリケーションでIDの持ち主に名前とアイコンが表示されるようにしたい場合、アプリ管理者は、Apple Business Registerを使用して登録し、正確なブランディング情報を提供する必要があります。送信した情報が正常に検証されると、トランザクションの時点でリーダー認証証明書が、リーダー認証証明書を介したApple Registerからのエンティティに関する情報をIDの持ち主に提供します。

iMessage

iMessageのセキュリティの概要

AppleのiMessageは、iPhoneおよびiPad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、リンクなどを添付することもでき、「いいね」のアイコンなどをメッセージに直接埋め込むことも可能です。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暗号化用の鍵ペアと署名用の鍵ペアが生成されます。暗号化には、RSA 1280ビットの鍵と、NIST P-256楕円曲線のEC 256ビットの暗号鍵が使用されます。署名には、ECDSA(楕円曲線デジタル署名アルゴリズム)の256ビットの署名鍵が使用されます。秘密鍵はデバイスのキーチェーンに保存され、初回のロック解除後にのみ使用できます。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。

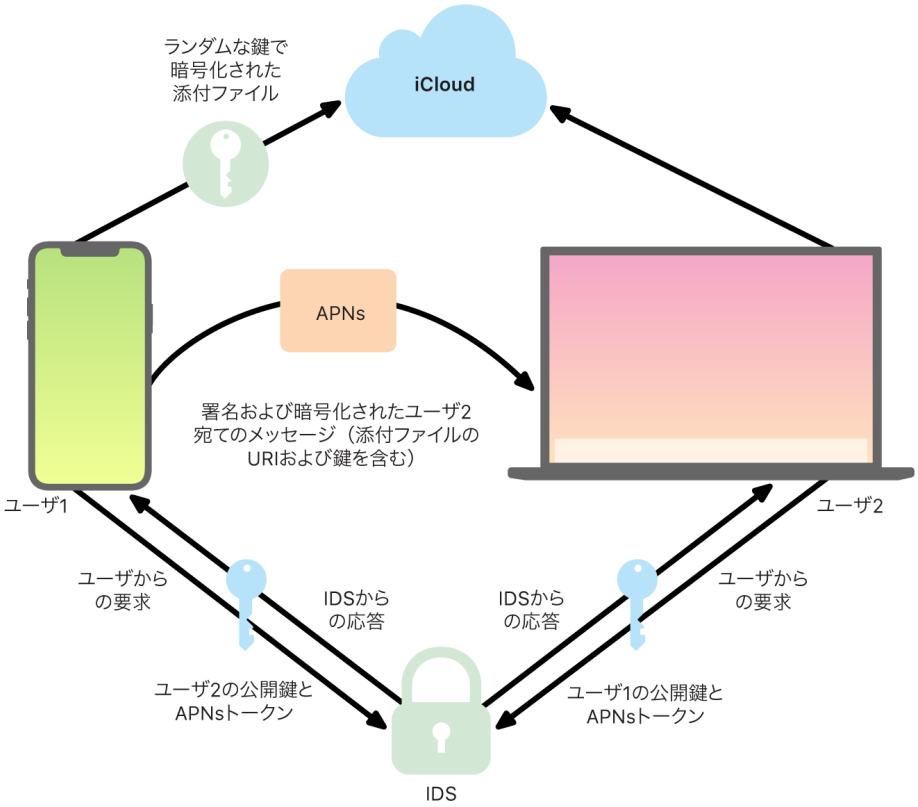
iMessageでのメッセージの安全な送受信方法

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Apple Identity Service(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あと、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。受信デバイスの暗号鍵と署名鍵は、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のカウンター(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整合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(楕円曲線デジタル署名アルゴリズム)の署名が付加されます。iOS 13以降およびiPadOS 13.1以降では、デバイスはRSA暗号化の代わりに楕円曲線統合暗号化スキーム(ECIES)暗号化を使用する場合があります。

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またはiPadOSのバージョンに応じて最大4または16 KB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、Uniform Resource Identifier(URI)、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。それらの機密性と整合性は、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情報と照合されます。

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Appleのサーバに最長30日間保存されます。

iMessageの安全な「名前と写真の共有」

iMessageの「名前と写真の共有」では、ユーザがiMessageを使って名前と写真を共有できます。ユーザはマイカードの情報を選択するか、名前をカスタマイズしたり自分で選んだ写真を含めたりできます。iMessageの「名前と写真の共有」では2ステージのシステムを使用して名前と写真が配信されます。

このデータはフィールド別に分割されて個別に暗号化および認証されると共に、以下のプロセスで全体が認証されます。次の3つのフィールドがあります。

- 名前
- 写真
- 写真ファイル名

データ作成の最初のステップでは、デバイス上で128ビットのレコードキーがランダムに生成されます。次に、HKDF-HMAC-SHA256によってこのレコードキーが導出され、Key 1:Key 2:Key 3 = HKDF（レコードキー、"nicknames"）という3つのサブキーが作成されます。ランダムな96ビットのIV（初期化ベクトル）がフィールドごとに生成され、AES-CTRおよびKey 1を使ってデータが暗号化されます。その後、Key 2を使って、フィールド名、フィールドのIV、フィールドの暗号テキストを秘匿してHMAC-SHA256でメッセージ認証コード（MAC）が計算されます。最後に、個別のフィールドのMAC値が連結され、そのMACがKey 3を使ってHMAC-SHA256で計算されます。暗号化されたデータと共に、この256ビットのMACが保存されます。このMACの最初の128ビットがRecordIDとして使用されます。

その後、この暗号化されたレコードがCloudKit公開データベースのRecordIDの下に保存されます。このレコードが変更（ミューテート）されることはなく、ユーザが自分の名前と写真の変更を選択したときは、新しい暗号化されたレコードがその都度生成されます。ユーザ1が自分の名前と写真をユーザ2と共有することを選択した場合、そのレコードキーがiMessageペイロード内のrecordIDと共に送信され、このペイロードが暗号化されます。

ユーザ2のデバイスがこのiMessageペイロードを受信すると、ペイロードにニックネームおよび写真のrecordIDと鍵が含まれることが通知されます。次に、ユーザ2のデバイスがCloudKit公開データベースにアクセスし、そのrecordIDの暗号化された名前と写真を取得して、iMessageを使用して転送します。

メッセージが取得されると、ユーザ2のデバイスはペイロードを復号し、recordID自体を使用して署名を検証します。検証に合格すると、名前と写真がユーザ2に表示され、ユーザ2はこれを自分の連絡先に追加するか、「メッセージ」で使用することを選択できます。

安全なApple Messages for Business

Apple Messages for Businessは、個人ユーザがメッセージアプリ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。Apple Messages for Businessを使用すると、ユーザは常にチャットをコントロールできます。ユーザがチャットを削除して、その企業や店舗から今後メッセージが届かないようにすることもできます。プライバシー保護のため、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。代わりに、Apple Identity Service（IDS）によって**不特定の識別情報**と呼ばれるカスタムの一意の識別情報が生成されて、企業や店舗と共有されます。不特定の識別情報は、ユーザのApple IDと企業や店舗のビジネスIDの関係ごとに一意になります。ユーザは、Apple Messages for Businessを使用して連絡を取る企業や店舗ごとに異なる不特定の識別情報を持ちます。個人を特定する情報を企業や店舗と共有するかどうかとそのタイミングはユーザが決定し、Apple Messages for Businessサービスがチャット履歴を保存することはありません。

Apple Messages for Businessでは、Apple Business Managerで作成された管理対象Apple IDがサポートされ、Apple School ManagerでiMessageおよびFaceTimeに対して管理対象Apple IDが有効になっているかどうかが判別されます。

企業や店舗に送信されるメッセージは、iMessageと同じセキュリティとAppleのメッセージングサーバを使用して、ユーザのデバイスとAppleのメッセージングサーバの間で暗号化されます。Appleのメッセージングサーバは RAM内のこれらのメッセージを復号し、TLS 1.2を使用して暗号化されたリンク経由で企業や店舗にリレーします。Apple Messages for Businessサービスを通過している間、メッセージが暗号化されていない形式で保存されることはありません。企業や店舗の返信も、TLS 1.2を使用してAppleのメッセージングサーバに送信され、そこで受信者のデバイスごとに一意の公開鍵を使って暗号化されます。

ユーザのデバイスがオンラインになっている場合、メッセージは即座に配信され、Appleのメッセージングサーバにはキャッシュされません。ユーザのデバイスがオンラインになっていない場合、暗号化されたメッセージは、デバイスが再度オンラインになったときにユーザが受信できるように最大30日間キャッシュされます。メッセージはデバイスが再度オンラインになるとすぐに配信され、キャッシュから削除されます。キャッシュされている未配信のメッセージは30日後に期限切れになり、完全に削除されます。

FaceTimeのセキュリティ

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)を使ってストリーミングされるメディアチャン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AES256を使用して暗号化され、HMAC-SHA1で認証されます。最初の接続とセキュリティの設定が行われたあとの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。グループFaceTimeでは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、これらのグループ通話には、Apple Identity Service(IDS)によって真正性が確保されることに加えて、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えいしません。セッション鍵はAES-SIVを使用してラップされ、P-256 ECDHの一時鍵による楕円曲線統合暗号化スキーム(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。

探す

「探す」のセキュリティ

Appleデバイス用の「探す」アプリは、公開鍵の高度な暗号化という基盤の上に構築されています。

概要

「探す」アプリは、「iPhoneを探す」と「友達を探す」をiOS、iPadOS、およびmacOS上で1つのアプリに統合したものです。「探す」では、紛失したデバイスを(オフラインのMacであっても)見つけることができます。デバイスがオンラインの場合は、その位置がiCloud経由でユーザに報告されます。「探す」は、付近で使用されているAppleデバイスで検出できる近距離Bluetooth信号を紛失したデバイスから送信することで、オフラインでも機能します。検出された紛失デバイスの位置情報が付近のデバイスによってiCloudにリレーされるため、関与するすべてのユーザのプライバシーとセキュリティを保護しつつ、ユーザは「探す」アプリでMacの位置を把握することができます。「探す」は、オフラインやスリープ状態のMacでも機能します。

ユーザはBluetoothと世界中で盛んに使用されている数百万台ものiOS、iPadOS、およびmacOSデバイスを使用して、紛失したデバイスがWi-FiまたはモバイルLTE通信ネットワークに接続できない場合でもそれを見つけることができます。「探す」の設定で「オフラインのデバイスを探す」が有効になっているすべてのiOS、iPadOS、またはmacOSデバイスが、「探知側デバイス」の役割を果たすことができます。つまり、デバイスはBluetoothを使用して、紛失した別のオフラインデバイスの存在を検出してから、自らのネットワーク接続を使用しておよその位置を所有者に報告できます。デバイスで「オフラインのデバイスを探す」が有効になっている場合、同じ方法で別の参加デバイスからそのデバイスを探せるということにもなります。このインタラクション全体はエンドツーエンドで暗号化され、匿名であり、バッテリーとデータを効率的に使用するように設計されています。バッテリー駆動時間やモバイルデータ通信プランの使用量への影響はごくわずかにとどまり、ユーザのプライバシーも保護されます。

注記: 「探す」は、国または地域によっては利用できないことがあります。

エンドツーエンドの暗号化

「探す」は公開鍵の高度な暗号化という基盤の上に構築されています。「探す」の設定で「オフラインのデバイスを探す」を有効にすると、{d,P}で表される楕円曲線(EC)P-224秘密鍵ペアがデバイス上で直接生成されます。この**d**は秘密鍵、**P**は公開鍵です。また、256ビットのシークレットSK_0が作成され、カウンター$_i$が0に初期化されます。この秘密鍵ペアとシークレットはAppleに送信されず、iCloudキーチェーンを使って、エンドツーエンドの暗号化された形でユーザのほかのデバイス間でのみ同期されます。シークレットとカウンタを使用して、現在の再帰構造「$SK_i = KDF(SK_{i-1}, \text{“update”})$」を持つ最新の対称鍵SKIが導出されます。

鍵SK_iに基づき、u_iとv_iの2つの長精度整数が $(u_i,v_i) = KDF(SK_i, \text{“diversify”})$で計算されます。次に、**d**で示されるP-224秘密鍵と、**P**で示される対応する公開鍵の両方が、2つの整数を含むアフィン関係を使用して導出され、短命の鍵ペアが計算されます: 導出される秘密鍵はd_iです。ここで、$d_i = u_i * d + v_i$(P-224曲線の位数を法とする)であり、対応する公開部分はP_iであり、$P_i = u_i*P + v_i*G$であることを検証します。

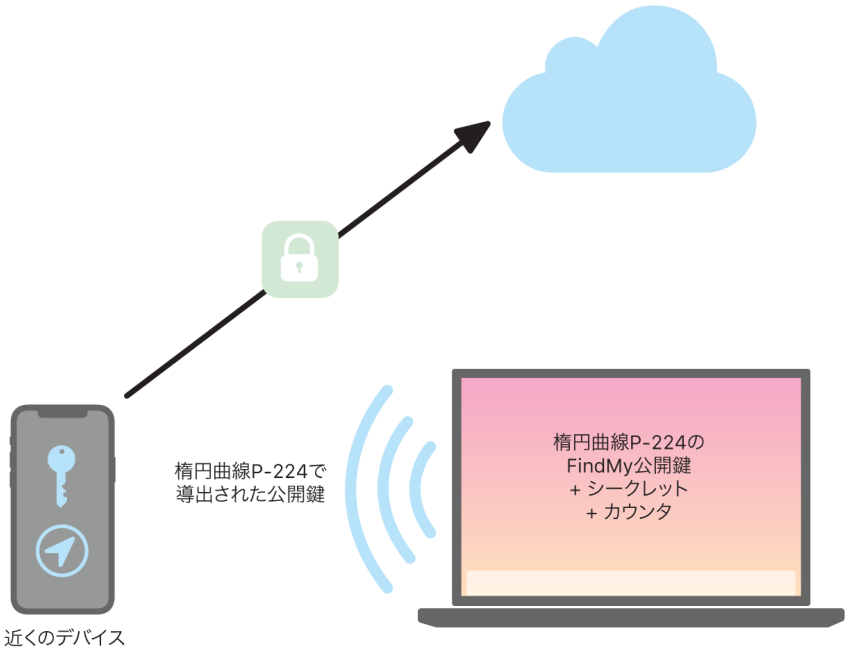
MacBook Proを公園のベンチに置き忘れたときなど、デバイスを紛失し、Wi-FiまたはモバイルLTE通信に接続できない場合、そのデバイスは一定期間、導出された公開鍵P_iのブロードキャストをBluetoothペイロード内で定期的に行います。P-224を使用することで、公開鍵表現を1つのBluetoothペイロードに収めることができます。周囲のデバイスはその位置情報を公開鍵で暗号化することで、オフラインデバイスの探索に貢献できます。約15分ごとに、カウンタの増分値と上記のプロセスを使用して公開鍵が新しいものに置き換えられるため、持続的な識別信号によってユーザが追跡されることはありません。この導出メカニズムは、さまざまな公開鍵P_iが同じデバイスにリンクされることを防止するように設計されています。

ユーザとデバイスの匿名性の確保

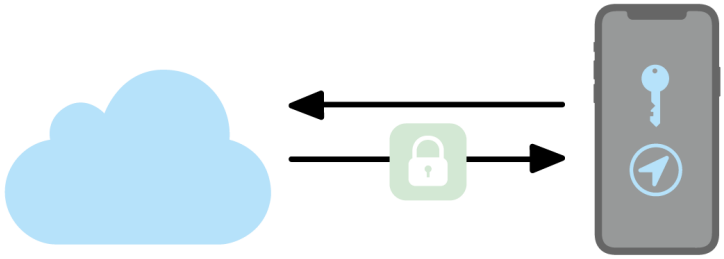
位置情報やその他のデータが必ず完全に暗号化されるだけでなく、参加するデバイスの識別情報もほかのデバイスやAppleに対して保護されます。探知側デバイスからAppleに送信されるトラフィックには、コンテンツにもヘッダにも認証情報が含まれません。そのため、探知側のユーザや見つかったデバイスの所有者がだれかをAppleが把握することはありません。さらに、Appleは探知側のユーザを識別する情報を記録せず、だれかが探知側のユーザと所有者を関連付けることができるような情報も保持しません。デバイスの所有者は暗号化された位置情報のみを受信します。この情報は復号されて「探す」アプリに表示されますが、だれがデバイスを見つけたかは示されません。

「探す」を使用して紛失したAppleデバイスを見つける

「オフラインのデバイスを探す」が有効になっていてBluetoothの通信圏内にあるAppleデバイスはすべて、「探す」を許可するように構成されている別のAppleデバイスからの信号を検出して、最新のブロードキャスト鍵P_iを読み取ることができます。探知側デバイスはECIES構成とブロードキャストから取得した公開鍵P_iを使って、自らの現在地の情報を暗号化してAppleにリレーします。暗号化された位置情報は、Bluetoothペイロードから取得されたP-224公開鍵P_iのSHA256ハッシュとして計算されるサーバインデックスに関連付けられます。Appleが復号鍵を入手することはないため、Appleは探知側で暗号化された位置情報を読み取ることはできません。紛失したデバイスの所有者はこのインデックスを再構築して、暗号化された位置情報を復号できます。



紛失したデバイスを探しているとき、位置情報の検索期間に予想されるカウンター値の範囲が推定されます。所有者側では、検索期間のカウンター値の範囲に含まれる元のP-224秘密鍵**d**とシークレット値SK_iを把握しているため、検索期間全体の値セット{d_i, SHA256(P_i)}を再構築できます。その後、紛失したデバイスを探すために使用されている所有者のデバイスが、インデックス値のセットSHA256(P_i)を使ってサーバへのクエリを実行し、暗号化された位置情報をサーバからダウンロードできます。次に「探す」アプリが、暗号化された位置情報を対応する秘密鍵d_iでローカルに復号し、紛失したデバイスのおよその位置をアプリ内に表示します。複数の探知側デバイスから送られた位置情報の報告が所有者のアプリによって統合され、より正確な位置情報が生成されます。



オフラインのデバイスを見つける

「iPhoneを探す」が有効になっているデバイスを使用しているユーザがデバイスをiOS 13以降、iPadOS 13.1以降、およびmacOS 10.15以降にアップグレードすると、デフォルトで「オフラインのデバイスを探す」が有効になります。これは、どのユーザにとっても、デバイスを紛失した場合に見つかる確率を可能な限り最大限に高めるためです。ただし、ユーザがこれに参加したくない場合は、デバイスの「探す」の設定で「オフラインのデバイスを探す」を無効にできます。「オフラインのデバイスを探す」を無効にすると、そのデバイスは探知側デバイスとして機能しなくなり、ほかの探知側デバイスから見つけられることもなくなります。ただし、この場合もデバイスはWi-Fiまたはモバイルデータ通信ネットワークに接続できるため、ユーザが見つけることはできます。

紛失したオフラインデバイスが見つかった場合、そのことを知らせる通知とメールメッセージがユーザに送信されます。紛失したデバイスの位置をユーザが表示するには、「探す」アプリを開いて「デバイス」タブを選択します。「探す」では、デバイスが見つかる前のように空白の地図上にデバイスが表示されるのではなく、デバイスがどのくらい前に検出されたかの情報とおよその住所が地図の場所と一緒に表示されます。位置情報の報告が増えるにつれ、現在地とタイムスタンプの両方が自動的にアップデートされます。ユーザはオフラインデバイスでサウンドを鳴らしたりオフラインデバイスをリモート消去したりすることはできませんが、デバイスを回収するために、位置情報を使って自分がたどってきた経路を戻るなどのアクションを実行できます。

連係機能

連係機能のセキュリティの概要

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。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のセキュリティ

AppleのHandoffは、デバイス間でも、ネイティブアプリとWebサイトの間でも安全に処理されます。大量のデータを渡す場合も同様です。

Handoffが安全に機能する仕組み

Handoffを使用すると、ユーザのiOS、iPadOS、およびmacOS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（BLE）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のメッセージ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BLE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AES256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初めて受信すると、発信元のデバイスとBLE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、BLE 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BLEではなくAPNsを使用して送信されます。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。

ネイティブアプリとWebサイトの間でのHandoff

Handoffを使用すると、iOS、iPadOS、およびmacOSのネイティブアプリで、そのアプリのデベロッパが正当に制御しているドメインのWebページでのユーザアクティビティを再開できます。また、ネイティブアプリ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アプリが要求できないようにするため、アプリは再開する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、アプリから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の受け入れをアプリに許可するには、アプリ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、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アプリが受け入れたことが検知され、そのネイティブアプリのアイコンがHandoffのオプションとして表示されます。そのネイティブアプリは、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アプリに渡されません。

また、Handoffを受け取るデバイスに同じネイティブアプリがインストールされていないときのために、ネイティブアプリはフォールバック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のアプリ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、要求した側のアプリ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、ネイティブアプリ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

一部のアプリでは、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と同様のもの）をサポートするAPIが使用されることもあります。例えば、メールアプリでは、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。

アプリでそれらのAPI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。ただし、受け取るデバイスは、Bluetooth Low Energy（BLE）を使用して最初のペイロードを受信したあとで、Wi-Fiで新しい接続を開始します。この接続は（TLSで）暗号化され、iCloudキーチェーンで共有される識別情報を経由して信頼を導出します。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、アプリ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。

アプリはユーザがクリップボードの内容をそのアプリ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）のアプリに拡張されます。

iPhone経由の通話のセキュリティ

Mac、iPad、またはHomePod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）を使って、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ユーザインターフェイスが表示されます。ユーザが電話に出ると、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（BLE）を使って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。

電話の発信もAPNsを使って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無効にできます。

iPhoneのSMS/MMS転送のセキュリティ

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または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iMessageのセキュリティの概要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送信メカニズ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のセキュリティ

Instant Hotspotは、ほかのAppleデバイスを個人用のiPhoneおよびiPadホットスポットに接続します。Instant Hotspotに対応しているiPhoneおよびiPadデバイスでは、Bluetooth Low Energy（BLE）を使用して、同じ個人のiCloudアカウントまたはファミリー共有で使用されているアカウントにサインインしているデバイス（iOS 13およびiPadOS）を検出し、通信します。OS X 10.10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iPhoneおよびiPadデバイスを検出し、通信します。

ユーザが最初にデバイスで「Wi-Fi」設定を開いたときに、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情報を含むBLEアドバタイズメントを発信します。この識別情報は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、Instant Hotspotが使用可能であることを示します。

ファミリー共有のメンバーではないユーザがインターネット共有に使用するiPhoneまたはiPad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、BLE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BLE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。

ファミリー共有のメンバーであるユーザについては、HomeKitデバイスで情報の同期に使用されるものと同様のメカニズムを使用して、インターネット共有接続の情報が安全に共有されます。特に、ユーザ間でインターネット共有の情報を共有する接続は、ユーザのデバイス固有のEd25519公開鍵で認証されるECDH（Curve25519）一時鍵で保護されます。使用される公開鍵は、ファミリー共有が確立されたときにIDSを使用してファミリー共有のメンバー間で同期されたものです。

ネットワークのセキュリティ

ネットワークのセキュリティの概要

Apple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もさまざまな手段があります。これにより、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。これらのセキュリティ機能や手段はすべてネットワークセキュリティに分類されます。

ユーザにとって、世界中どこからでも企業のネットワークにアクセスできることは不可欠であるため、ユーザの認証と、データ転送時の保護を確実に行うことが重要です。iOS、iPadOS、およびmacOS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。こうした理由から、Appleのオペレーティングシステムは、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。

TLSのセキュリティ

iOS、iPadOS、およびmacOSは、Transport Layer Security（TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3）およびDatagram Transport Layer Security（DTLS）に対応しています。TLSプロトコルは、AES128とAES256の両方をサポートし、前方秘匿性を持つ暗号スイートを優先します。Safari、カレンダー、メールなどのインターネットアプリは、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暗号化された通信チャネルを有効にします。ハイレベルAPI（CFNetworkなど）を使うことで、TLSをアプリに簡単に導入できるほか、低レベルAPI（Network.frameworkなど）を使ったきめ細かい制御も可能です。CFNetworkはSSL 3の使用を許可せず、WebKitを使用するアプリ（Safariなど）はSSL 3接続の確立が禁止されます。

iOS 11以降およびmacOS 10.13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 10.12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が唯一の暗号スイートの場合は、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アプリをアップグレードして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において、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ログとして記録されている必要があります。iOS 12.2では、Network.framework APIとNSURLSession APIでTLS 1.3がデフォルトで有効になります。SecureTransport APIを使用するTLSクライアントは、TLS 1.3を使用できません。

App Transport Security

アプリ 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、アプリ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、前方秘匿性を持つ以下の暗号スイートのみに限定しています。

- Galois/Counter Mode(GCM)でのECDHE_ECDSA_AESおよびECDHE_RSA_AES
- CBC(暗号ブロック連鎖)モード

アプリ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にRSA_AESが追加されます。

サーバはTLS 1.2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SHA256以上を使って署名された有効な証明書も必要です。

アプリがアプリ Transport Securityを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。アプリ Transport SecurityはiOS 9以降およびmacOS 10.11以降向けにコンパイルされたアプリに自動的に適用されます。

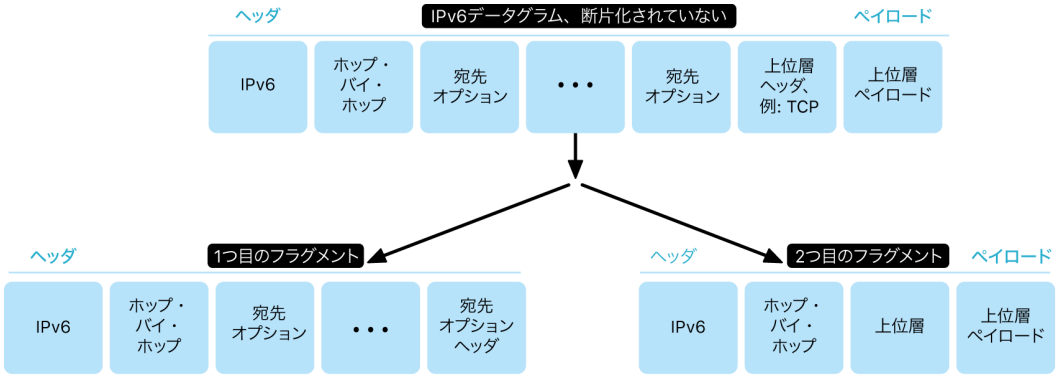
証明書の有効性チェック

TLS証明書の信頼評価は、RFC 5280に定められた確立済みの業界標準に従って行われ、RFC 6962(証明書の透明性)などの新しい標準規格も採用されています。iOS 11以降およびmacOS 10.13以降のAppleデバイスでは、失効および制限されている証明書の最新リストが定期的にアップデートされます。このリストは、Appleが信頼する組み込み済みの各ルート認証局とその下位の認証局が公開する証明書失効リスト(CRL)から生成されます。このリストには、Appleの判断によるその他の制限が含まれる場合もあります。安全な接続を確立するためにネットワークAPIが使用されるときは、常にこの情報が参照されます。認証局が個別にリストする失効済みの証明書が多すぎる場合は、信頼評価にオンライン証明書状況プロトコル(OCSP)の応答が必要になることがあり、この応答が得られないと信頼評価は失敗に終わります。

IPv6のセキュリティ

Appleのすべてのオペレーティングシステムは IPv6をサポートし、ユーザのプライバシー保護とネットワーキングスタックの安定性のために複数のメカニズムを実装しています。ステートレスアドレス自動構成(SLAAC)が使用される場合、ネットワーク越しのデバイスのトラッキングを防止するのと同時に、ネットワークが変更されない場合のアドレス安定性を保証することでユーザの体験を向上させるような方法で、すべてのインターフェイスのIPv6アドレスが生成されます。アドレス生成アルゴリズムはRFC 3972の時点での暗号生成アドレスに基づいています。これはインターフェイス固有の修飾子によって拡張され、同じネットワーク上の異なるインターフェイスも最終的に異なるアドレスを持つことが保証されています。また、一時アドレスは24時間の推奨有効期間で作成され、これらはデフォルトで新しい接続に使用されます。iOS 14、iPadOS 14、およびwatchOS 7で導入されたプライベートWi-Fiアドレス機能に合わせて、デバイスが接続するすべてのWi-Fiネットワークに対して一意のリンクローカルアドレスが生成されます。ネットワークのSSIDはアドレス生成のための追加要素として組み込まれます。これはRFC 7217時点でのNetwork_IDパラメータと同様です。この方法はiOS 14、iPadOS 14、およびwatchOS 7で使用されています。

Appleデバイスでは、IPv6拡張ヘッダおよびフラグメンテーションに基づく攻撃から保護するため、RFC 6980、RFC 7112、およびRFC 8021に規定された保護対策を実装しています。ほかにも対策はありますが、これらが特に阻止する攻撃は、上位層ヘッダが2番目のフラグメントでのみ見つかるため(以下を参照)、ステートレスパケットフィルタなどのセキュリティ制御があいまいになる可能性があるものです。



さらに、Appleのオペレーティングシステムの iPv6スタックの信頼性を保証するために、Appleデバイスは、IPv6関連のデータ構造にさまざまな制限(インターフェイスごとのプレフィックスの数など)を適用します。

VPN（仮想プライベートネットワーク）のセキュリティ

仮想プライベートネットワーク（VPN）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、iPhone、iPad、およびMacデバイスで使用できるようになります。

サポートされるプロトコル

これらのデバイスは、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、楕円曲線デジタル署名アルゴリズム（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アプリを使用）
- L2TP/IPsec（MS-CHAPV2パスワードによるユーザ認証と、共有シークレット（iOS、iPadOS、macOS）およびRSA SecurIDまたはCRYPTOCard（macOSのみ）によるコンピュータ認証）
- Cisco IPsec（パスワード、RSA SecurID、またはCRYPTOCardによるユーザ認証と、共有シークレットおよび証明書によるコンピュータ認証（macOSのみ））

サポートされるVPN導入

iOS、iPadOS、およびmacOS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。モバイルデバイス管理（MDM）ソリューションでは、各管理対象アプリやSafariの特定のドメインが使用する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。

iOSとiPadOSでは、次の接続がサポートされます:

- **VPN常時接続:** MDMソリューションで管理され、Mac用Apple Configurator、Apple School Manager、Apple Business Manager、またはApple Business Essentialsで監視されているデバイス用です。VPN常時接続により、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、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。以降の暗号化のためのパラメータと鍵のデフォルト交換方式であるIKEv2は、データ暗号化を使用してトラフィック送信を保護します。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のセキュリティ

ワイヤレスネットワークへの安全なアクセス

Appleのプラットフォームはすべて業界標準のWi-Fi認証および暗号化プロトコルに対応しており、以下の安全なワイヤレスネットワークへの接続時に、認証を用いたアクセスと機密保持が可能になります:

- WPA2パーソナル
- WPA2エンタープライズ
- WPA2 /WPA3 Transitional
- WPA3パーソナル
- WPA3エンタープライズ
- WPA3エンタープライズ192ビットセキュリティ

WPA2およびWPA3によって各接続が認証され、128ビットのAES暗号化が行われるため、ワイヤレスで送信されるデータの機密が保証されます。そのため、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。

WPA3サポート

WPA3は以下のAppleデバイスでサポートされます:

- iPhone 7以降
- iPad第5世代以降
- Apple TV 4K以降
- Apple Watch Series 3以降
- Macコンピュータ(Late 2013以降、802.11ac以降に対応)

最近のデバイスは、WPA3エンタープライズ192ビットセキュリティによる認証に対応しています。これには、対応するワイヤレスアクセスポイント(AP)に接続する場合の256ビットAES暗号化への対応が含まれます。この暗号化によって、ワイヤレスで送信されるトラフィックの機密保護が一層強化されます。WPA3エンタープライズ192ビットセキュリティは、すべてのiPhone 11以降のモデル、iPad第7世代以降のすべてのiPadモデル、Appleシリコンを搭載したすべてのMacコンピュータが対応しています。

PMFサポート

ワイヤレスで送信されるデータの保護に加え、Appleのプラットフォームは802.11wで定義されているProtected Management Frame(PMF、管理フレーム保護)サービスを通じて、WPA2およびWPA3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のサポートは以下のAppleデバイスで利用可能です:

- iPhone 6以降
- iPad Air 2以降
- Apple TV HD以降
- Apple Watch Series 3以降
- Macコンピュータ(Late 2013以降、802.11ac以降に対応)

また、Appleデバイスは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。サポートされる802.1Xワイヤレス認証方法には、EAP-TLS、EAP-TTLS、EAP-FAST、EAP-SIM、PEAPv0、およびPEAPv1があります。

プラットフォームの保護

Appleのオペレーティングシステムはデバイスをネットワークプロセッサのファームウェアにある脆弱性から保護します。これにより、Wi-Fi付きのネットワークコントローラはアプリケーションプロセッサのメモリへのアクセスを制限されます。

- 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（セキュアデジタルI/O）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バスの入出力メモリ管理ユニット（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および制御構造を含むメモリおよびリソースのみにさらに制限されます。

非推奨のプロトコル

Apple製品は、以下の非推奨のWi-Fi認証および暗号化プロトコルに対応しています:

- WEP Open（40ビット鍵使用および104ビット鍵使用の両方）
- WEP Shared（40ビット鍵使用および104ビット鍵使用の両方）
- ダイナミックWEP
- 一時鍵統合プロトコル（TKIP）
- WPA
- WPA/WPA2 Transitional

これらのプロトコルは安全と見なされなくなったため、互換性、信頼性、パフォーマンス、およびセキュリティ上の理由により、利用しないことが強く推奨されます。これらは下位互換性を確保する目的でのみサポートされており、将来のソフトウェアバージョンでは削除される可能性があります。

可能な限り最高の堅牢性、セキュリティ、および互換性を備えたWi-Fi接続を提供できるように、Wi-Fiのすべての実装をWPA3パーソナルまたはWPA3エンタープライズに移行することをおすすめします。

Wi-Fiのプライバシー

MACアドレスのランダム化

Appleのプラットフォームは、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（メディアアクセス制御アドレス）を使用します。このようなスキャンは、既知の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アプリ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Appleのマップアプリ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。Wi-Fi MACアドレスのランダム化は、iPhone 5以降でサポートされています。

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、Appleのプラットフォームは、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アプリ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およびiPadOSのWi-Fiスキャンがランダムな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。

iOS 14以降、iPadOS 14以降、およびwatchOS 7以降では、iPhone、iPad、またはApple WatchがWi-Fiネットワークに接続すると、各ネットワークで一意の（ランダム化された）MACアドレスでそれ自体を識別します。この機能は、ユーザが無効にすることも、Wi-Fiペイロードの新しいオプションを使用して無効にすることもできます。特定の状況下では、デバイスは実際のMACアドレスにフォールバックします。

詳しくは、Appleサポートの記事「iPhone、iPad、Apple WatchでプライベートWi-Fiアドレスを使う」を参照してください。

Wi-Fiフレームのシーケンス番号のランダム化

Wi-Fiフレームにはシーケンス番号があります。これは、効率的で信頼性の高いWi-Fi通信を可能にするために、低レベルの802.11プロトコルで使用されます。このシーケンス番号は1フレーム送信されるたびに増分されるため、Wi-Fiスキャン時に送信される情報と、同じデバイスによって送信されるその他のフレームを関連付けるために使用されるおそれがあります。

これを防止するため、Appleデバイスではいずれかの MACアドレスが新しいランダムなアドレスに変更されるたびに、このシーケンス番号もランダム化されます。その一環として、デバイスが関連付けられていないときに新たなスキャン要求が開始されるたびに、シーケンス番号がランダム化されます。このランダム化は以下のデバイスでサポートされます。

- iPhone 7以降
- iPad第5世代以降
- Apple TV 4K以降
- Apple Watch Series 3以降
- iMac Pro（Retina 5K、27インチ、2017）以降
- MacBook Pro（13インチ、2018）以降
- MacBook Pro（15インチ、2018）以降
- MacBook Air（Retina、13インチ、2018）以降
- Mac mini（2018）以降
- iMac（Retina 4K、21.5インチ、2019）以降
- iMac（Retina 5K、27インチ、2019）以降
- Mac Pro（2019）以降

Wi-Fi接続

Appleは、AirDropおよびAirPlay用のピアツーピアWi-Fi接続のために、ランダム化されたMACアドレスを生成します。ランダム化されたアドレスは、iOSおよびiPadOS（SIMカード搭載）でのインターネット共有と、macOSでのインターネット共有でも使用されます。

これらのネットワークインターフェイスが起動するたびに新しいランダムなアドレスが生成され、必要に応じてインターフェイスごとに一意のアドレスが個別に生成されます。

非公開ネットワーク

Wi-Fiネットワークは**サービスセット識別名（SSID）**と呼ばれるネットワーク名で識別されます。一部のWi-FiネットワークはSSIDを公開しないように構成されます。この場合、ワイヤレスアクセスポイントはネットワークの名前をブロードキャストしません。これらは**非公開ネットワーク**と呼ばれます。iPhone 6s以降のデバイスではネットワークが非公開になっている場合に自動で検出します。ネットワークが非公開の場合、iOSまたはiPadOSデバイスはこの要求時にSSIDを含めたプローブを送信します。ネットワークが非公開でなければ送信しません。これによって、以前にユーザが接続していた非公開ネットワークの名前をデバイスがブロードキャストすることが防止されるため、より一層プライバシーが保護されます。

Bluetoothのセキュリティ

Appleデバイスでは、Bluetooth ClassicとBluetooth Low Energy（BLE）の2種類のBluetoothが使用されます。両バージョンのBluetoothセキュリティモデルは、以下の固有のセキュリティ機能を備えています。

- ペアリング: 1つ以上の共有秘密鍵を作成するプロセス
- ボンディング: 信頼できるデバイスペアを構築するために、ペアリング時に作成された鍵を後続の接続用に保存すること
- 認証: 2台のデバイスが同じ鍵を持っていることの確認
- 暗号化: メッセージの機密保持
- メッセージの整合性: メッセージの偽造からの保護
- セキュアシンプルペアリング: 受動的盗聴からの保護と中間者攻撃からの保護

Bluetoothバージョン4.1ではBluetooth Classic（BR/EDR）物理トランスポートにセキュア接続機能が追加されました。

各種Bluetoothのセキュリティ機能は以下の通りです。

サポート	Bluetooth Classic	Bluetooth Low Energy
ペアリング	P-256楕円曲線	FIPS認定アルゴリズム（AES-CMACおよびP-256楕円曲線）
ボンディング	ペアリングの情報をiOS、iPadOS、macOS、tvOS、およびwatchOSデバイス上の安全な場所に保存	ペアリングの情報をiOS、iPadOS、macOS、tvOS、およびwatchOSデバイス上の安全な場所に保存
認証	FIPS認定アルゴリズム（HMAC-SHA256およびAES-CTR）	FIPS認定アルゴリズム
暗号化	コントローラによって実行されるAES-CCM暗号化	コントローラによって実行されるAES-CCM暗号化
メッセージの整合性	メッセージの整合性確保のために使用されるAES-CCM	メッセージの整合性確保のために使用されるAES-CCM
セキュアシンプルペアリング: 受動的盗聴からの保護	楕円曲線Diffie-Hellman一時鍵共有（ECDHE）	楕円曲線Diffie-Hellman鍵共有（ECDHE）
セキュアシンプルペアリング: 中間者（MITM）攻撃からの保護	ユーザが支援する2つの数値法: 数値比較およびパスキー入力	ユーザが支援する2つの数値法: 数値比較およびパスキー入力 MITM以外のすべてのペアリングモードを含め、ペアリングにユーザの応答が必要
Bluetooth 4.1以降	iMac Late 2015以降 MacBook Pro Early 2015以降	iOS 9以降 iPadOS 13.1以降 macOS 10.12以降 tvOS 9以降 watchOS 2.0以降
Bluetooth 4.2以降	iPhone 6以降	iOS 9以降 iPadOS 13.1以降 macOS 10.12以降 tvOS 9以降 watchOS 2.0以降

Bluetooth Low Energyのプライバシー

ユーザのプライバシーを保護するため、BLEはアドレスのランダム化とトランスポート間での鍵導出という2つの機能を備えています。

アドレスのランダム化は、Bluetoothデバイスのアドレスを頻繁に変更することで一定期間内にBLEデバイスが追跡される可能性を低減する機能です。このプライバシー機能を使用しているデバイスが既知のデバイスに再接続するには、**プライベートアドレス**と呼ばれるデバイスのアドレスを他方のデバイスで解決できるようにする必要があります。プライベートアドレスは、ペアリング手順で交換されるデバイスのID解決鍵を使って生成されます。

iOS 13以降およびiPadOS 13.1以降には、トランスポート間でリンク鍵を導出する機能があります。これは、**トランスポート間の鍵導出**と呼ばれる機能です。例えば、BLEで生成されたリンク鍵を使ってBluetooth Classicのリンク鍵を導出することができます。また、AppleはBluetoothコア仕様4.1で導入されたセキュア接続機能(Bluetoothコア仕様5.1を参照)に対応するデバイスについて、BLEをサポートするためにBluetooth Classicを追加しました。

iOSの超広帯域無線のセキュリティ

Appleが設計した新しいU1チップでは、空間認識のために超広帯域無線テクノロジーが使用されます。これにより、iPhone 11、iPhone 11 Pro、およびiPhone 11 Pro Max以降のiPhoneモデルでU1を搭載したほかのAppleデバイスの位置を正確に特定できます。超広帯域無線テクノロジーでは、サポートされるほかのAppleデバイスに備わっているものと同じデータのランダム化技術が使用されます。

- MACアドレスのランダム化
- Wi-Fiフレームのシーケンス番号のランダム化

シングルサインオンのセキュリティ

シングルサインオン

iOSとiPadOS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、他社製アプリで使用できます。証明書ベースの認証（PKINITなど）にも対応しています。

macOSでは、企業ネットワークへの認証にKerberosを使用できます。アプリは、アクセスを承認されているサービスに対するユーザ認証にKerberosを使用できます。Kerberosは、幅広い範囲のネットワークアクティビティにも利用することができ、Safariの安全なセッションや、他社製アプリに対するネットワークファイルシステムの認証で使用できます。証明書ベースの認証にも対応しています。ただし、アプリでデベロッパAPIが採用されている必要があります。

iOS、iPadOS、およびmacOSのSSOは、SPNEGOトークンとHTTP Negotiateプロトコルを使用して、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。

iOS、iPadOS、およびmacOSでは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およびiPadOSネットワークAPIを使用する他社製アプリも、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およびiPadOSは構成プロファイルペイロードをサポートしており、これによりモバイルデバイス管理（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の使用を許可するアプリとSafariのWeb URLの設定が含まれます。

拡張シングルサインオン

アプリデベロッパはSSO機能拡張を使って独自のシングルサインオンの実装を提供できます。SSO機能拡張は、ネイティブアプリまたはWebアプリでユーザ認証のために何らかのIDプロバイダを利用する必要がある場合に呼び出されます。デベロッパは、HTTPSへのリダイレクトと、Kerberosなどのチャレンジ/応答メカニズムの使用という2種類の機能拡張を提供できます。これによって、拡張シングルサインオンがOpenID、OAuth、SAML2、およびKerberosの認証スキームに対応します。また、SSO機能拡張は、ネイティブSSOプロトコルを採用することでmacOSの認証にも対応できます。このプロトコルは、macOSログイン中にSSOトークンの取得を可能とするものです。

アプリはシングルサインオン機能拡張を利用するために、AuthenticationServices APIを使用するか、オペレーティングシステムから提供されるURLインターセプションメカニズムに頼ることができます。WebKitとCFNetworkは、任意のネイティブアプリまたはWebKitアプリでシングルサインオンへのシームレスな対応を許可するインターセプションレイヤーを提供します。シングルサインオン機能拡張を呼び出すには、管理者から提供された構成がモバイルデバイス管理（MDM）プロファイルを介してインストールされている必要があります。さらに、リダイレクトタイプの機能拡張では関連ドメインペイロードを使用して、その機能拡張に対応するIDサーバに自らの存在が認識されていることを証明する必要があります。

オペレーティングシステムで提供されている機能拡張はKerberos SSO機能拡張のみです。

AirDropのセキュリティ

AirDropをサポートするApple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、AirDropに対応するiOS 7以降を搭載したiOSデバイスおよびiPadデバイスやOS X 10.11以降を搭載した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ワイヤレスアクセスポイント（AP）を使用せずにデバイス間で直接通信します。この接続はTLSで暗号化されます。

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。組織は、モバイルデバイス管理（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アプリでAirDropの使用を制限できます。

AirDropの動作

AirDropではユーザの認証を円滑に行うためにiCloudサービスを使用します。ユーザがiCloudにサインインすると、2048ビットのRSA識別情報がデバイスに保存されます。ユーザがAirDropをオンにすると、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、短いAirDrop識別情報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、送信側のデバイスがBLE経由で、ユーザの短いAirDrop識別情報ハッシュを含む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Appleデバイスが近くにあり、そのデバイスがこの信号を検出してピアツーピアWi-Fiを使用して応答すると、送信デバイスは、応答側のデバイスの識別情報を検出できます。

「連絡先のみ」モードでは、受信デバイスで、受信した短いAirDrop識別情報ハッシュが、連絡先アプリの登録者のハッシュと照合されます。一致が見つかると、受信デバイスは、ピアツーピアWi-Fiを介して応答し、その識別情報を伝えます。一致が見つからない場合、デバイスは応答しません。

「すべての人」モードでも、全体的なプロセスは同じです。ただし、受信デバイスの連絡先アプリで一致が見つからなくても受信デバイスが応答します。

それを受けて、送信デバイスは、ピアツーピアWi-Fiを使用してAirDrop接続を開始し、この接続を介して長い識別情報ハッシュを受信デバイスに送信します。受信デバイスは、この長い識別情報ハッシュと、「連絡先」で検出した登録者のハッシュを照合し、一致すると、長い識別情報ハッシュを返します。

ハッシュが確認されると、受信者の下の名前と写真（「連絡先」にある場合）が送信デバイスのAirDropの共有シートに表示されます。iOSおよびiPadOSデバイスでは、これらは「知っている人」セクションまたは「デバイス」セクションに表示されます。確認または認証されていないデバイスは、送信者のAirDropの共有シートにシルエットアイコンとデバイス名（「設定」>「一般」>「情報」>「名前」で定義）で表示されます。iOSおよびiPadOSでは、AirDropの共有シートの「その他の人」セクションに表示されます。

その後、送信ユーザが共有したい相手を選択できます。ユーザが選択すると、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。

証明書が確認されると、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。

iPhoneおよびiPadでのWi-Fiパスワードの共有のセキュリティ

Wi-Fiパスワードの共有に対応するiPhoneおよびiPad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。

ユーザがいずれかのWi-Fiネットワーク（リクエスト側）を選択してその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（BLE）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Appleデバイスが近くにある場合、そのデバイスはBLE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パスコードを送信します。これはネットワークへの接続に使用できます。

組織は、モバイルデバイス管理（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アプリでのWi-Fiパスワード共有の使用を制限できます。

macOSのファイアウォールのセキュリティ

macOSには、ネットワークアクセスおよびDOS（denial-of-service）攻撃からMacを保護するためのファイアウォールが組み込まれています。これは、「システム設定」>「プライバシーとセキュリティ」（macOS 13以降）または「システム環境設定」の「セキュリティとプライバシー」パネル（macOS 12以前）で設定できます。また、手動でインストールしたまたはMDMソリューションから提供されたファイアウォールペイロードを含む構成プロファイルを使用して設定することもできます。以下の構成に対応しています:

- アプリにかかわらず外部からの接続をすべてブロックする。
- 内蔵ソフトウェアが外部からの接続を受け入れるのを自動的に許可する。
- ダウンロードされた署名付きソフトウェアが外部からの接続を受け入れるのを自動的に許可する。
- ユーザが指定したアプリに基づきアクセスを追加または拒否する。
- MacがICMP（インターネット制御メッセージプロトコル）プローブおよびポートスキャン要求に応答することを禁止する。

デベロッパキットのセキュリティ

デベロッパキットのセキュリティの概要

Appleは、社外のデベロッパがAppleのサービスを拡張できるよう、数多くの「キット」フレームワークを提供しています。以下のフレームワークは、ユーザのプライバシーとセキュリティを核に据えて作成されています。

- HomeKit
- CloudKit
- SiriKit
- WidgetKit
- DriverKit
- ReplayKit
- ARKit

HomeKitのセキュリティ

HomeKitの通信のセキュリティ

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とデバイスのセキュリティ機能を使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、ユーザのデバイス上で生成され、これがそのユーザのHomeKit識別情報となります。この鍵ペアをHomeKitアクセサリプロトコル（HAP）の一部として使用して、ユーザのAppleデバイスとユーザのHomeKitアクセサリ間での直接の通信が認証されます。

ホームハブのあるホームでは、共有ホームのメンバーがこのホームハブを通じてアクセサリにコマンドを送信できます。これらのコマンドは、Apple Identity Service（IDS）を使用して、ユーザのデバイスからホームハブに送信され、エンドツーエンドで暗号化、および認証されます。そしてホームハブから、HomeKitアクセサリプロトコル（HAP）またはスマートホーム接続の規格であるMatterを使用して、関連するアクセサリにコマンドが転送されます。

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。iCloudキーチェーンを使用して、鍵はデバイス間で最新の状態に保たれます。

HomeKit対応アクセサリ間の通信

HomeKit対応アクセサリは、Apple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。

Apple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の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-SHA512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-SHA512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（BLE）の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に対応したBLEデバイスの場合、ペアリングされたデバイスが、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BLEアドバタイズを使用して通知される、アクセサリの状態変化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-SHA512から導出された鍵であり、データはChaCha20-Poly1305 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定期的に変更され、iCloudを使用してほかのデバイスでアップデートされます（「HomeKitデータのセキュリティ」を参照してください）。

Matter対応アクセサリとの通信

Matter対応アクセサリの識別情報とセキュリティは、証明書に基づいています。Appleホームでは、信頼の起点である認証局（CA）が最初のユーザ（所有者）のデバイスで生成され、CAの秘密鍵は所有者のiCloudキーチェーンに保存されます。ホームのそれぞれのAppleデバイスは、NIST P256を使用して証明書署名要求（CSR）を生成します。このCSRを取り込んだ所有者のデバイスは、所有者のCA秘密鍵を使用して、デバイスのMatter ID証明書を作成します。次に、この証明書を使用して、ユーザのデバイスとアクセサリ間の通信が認証されます。

Matter対応アクセサリは固有のNIST P256鍵ペアとCSRを生成し、アクセサリのペアリング中にCAから証明書を受け取ります。鍵ペアの生成前に、Matter対応アクセサリとホーム所有者のデバイスは（アクセサリメーカーが提供したPINとSPAKE2+プロトコルを使用して）鍵を交換し、デバイス認証プロセスが行われます。そして、このチャンネルを通してCSRと証明書が交換されます。暗号化には、HKDF-SHA256から導出された鍵を用いたAES-CCMが使用されます。アクセサリが工場出荷時の設定に復元されると、新しい鍵ペアとCSRが生成され、ペアリング中にアクセサリの新しい証明書が発行されます。

使用時にAppleデバイスとMatter対応アクセサリが通信する場合は、固有の証明書を使用して互いに認証します。各セッションは、三段階の（シグマ）プロトコルによって確立され、セッションごとのP256鍵に基づいてHKDF-SHA256から導出された鍵で暗号化されます。

AppleデバイスがMatter対応アクセサリと安全にやりとりする方法について詳しくは、Apple DeveloperのWebサイトの「iOS 16でのMatter対応」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。

Siri対応HomeKitアクセサリ

ユーザはSiri対応アクセサリでホームアプリを使用して、Siriなどの新しい機能や、タイマー、アラーム、インターコム、ドアベルなどのその他のHomePodの機能を有効にできます。これらの機能が有効になると、アクセサリは、これらのApple機能をホストするローカルネットワーク上のペアリングされたHomePodと連係します。デバイス間のオーディオの交換は、HomeKitとAirPlayの両方のプロトコルを使用して、暗号化されたチャンネル上で行われます。

「"Hey Siri"を聞き取る」がオンになっている場合は、アクセサリはローカルで実行されるトリガーフレーズ検知エンジンを使用して「Hey Siri」フレーズを聞き取ります。このエンジンがフレーズを検知すると、ペアリングされたHomePodにオーディオフレームがHomeKitを使用して直接送信されます。HomePodはオーディオを再度チェックし、フレーズにトリガーフレーズが含まれないと判断した場合はオーディオセッションをキャンセルする場合があります。

「タッチして起動」がオンになっている場合は、ユーザはアクセサリにある専用のボタンを押すことでSiriと会話を始めることができます。オーディオフレームはペアリングされたHomePodに直接送信されます。

Siriの呼び出しに成功したことが検知されると、HomePodはオーディオをSiriのサーバに送信し、HomePod自体をユーザが呼び出した場合にHomePodが適用するのと同じセキュリティ、プライバシー、暗号化保護を使用して、ユーザの意図を実現します。Siriがオーディオで返事をすると、Siriの応答はAirPlayオーディオチャンネルを通じてアクセサリに送信されます。一部のSiriリクエストには、ユーザからの追加の情報が必要です（ユーザがさらにオプションを聞きたいか質問するなど）。その場合、アクセサリはユーザに質問するという指示を受け取り、追加のオーディオがHomePodにストリーミングされます。

アクセサリには、聞き取り中であることをユーザに視覚的に示すものが必要です（LEDインジケータなど）。オーディオストリームへのアクセスを除いて、アクセサリにはSiriリクエストの意図は知らされず、アクセサリ上にユーザデータは保存されません。

HomeKitデータのセキュリティ

新しいHomeKitアーキテクチャ（iOS 16.2およびiPadOS 16.2で使用可能）にアップグレードされたホームでは、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Appleデバイス間で安全に同期されます。このプロセス中、HomeKitデータはiCloudのエンドツーエンドの暗号化を使用して暗号化され、Appleはアクセスできません。

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（所有者）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。

ホームデータとアプリ

アプリ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。アプリ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/iPadOS/macOS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アプリからアクセスできるようになります。詳しくは、https://developer.apple.com/homekit/（英語）にあるHomeKitデベロッパ向けドキュメントを参照してください。

ローカルデータストレージ

HomeKitはユーザのApple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。このデータは、Protected Until First User Authenticationのデータ保護クラスを使用してData Vault内に保存されます。HomeKitデータはローカルのバックアップではバックアップされません。

HomeKitでのルーターの保護

ユーザは、HomeKit対応のルーターを使用することでホームネットワークのセキュリティを強化できます。これらのルーターを使用すると、HomeKit対応アクセサリによるローカルネットワークやインターネットへのWi-Fiアクセスを管理することができます。これらのルーターはプライベートPSK（PPSK）認証にも対応しているので、アクセサリ固有の鍵を使用してアクセサリをWi-Fiネットワークに追加したり、必要に応じてアクセサリを取り消したりできます。PPSK認証により、メインのWi-Fiパスワードがアクセサリに開示されないためセキュリティが強化され、ルーターのMACアドレスが変わってもルーターは安全にアクセサリを識別できます。

ホームアプリを使用して、ユーザはアクセサリのグループに対して以下のようなアクセス制限を設定できます:

- 制限なし: インターネットとローカルネットワークに無制限でアクセスできます。
- 自動: これがデフォルトの設定です。アクセサリメーカーからAppleに提供されたインターネットサイトとローカルポートのリストに基づき、インターネットとローカルネットワークへのアクセスが許可されます。このリストには、アクセサリが正常に機能するために必要なすべてのサイトとポートが含まれます。（このようなリストが利用可能になるまでは「制限なし」に設定されます。）
- ホームに制限: HomeKitがローカルネットワーク（リモートコントロールをサポートするためのホームハブを含む）からアクセサリを検出したり、制御したりするために必要な接続を除き、インターネットまたはローカルネットワークにアクセスしません。

PPSKは強力なアクセサリ固有のWPA2パーソナルのパスフレーズで、HomeKitによって自動的に生成され、あとでアクセサリが「ホーム」から削除されると取り消されます。HomeKitルーターが設定されている「ホーム」でHomeKitによってアクセサリがWi-Fiネットワークに追加されるときには、PPSKが使用されます。この追加はホームアプリのアクセサリの設定画面に「Wi-Fi資格情報: **HomeKit管理対象**」として反映されます。ルーターを追加する前にWi-Fiネットワークに追加されたアクセサリは、PPSKに対応している場合はPPSKを使用するために再構成されます。対応していない場合は既存の資格情報を保持します。

追加のセキュリティ対策として、ユーザはルーターメーカーのアプリを使ってHomeKit対応ルーターを設定して、ユーザがそのルーターにアクセスできること、およびホームアプリにそのルーターを追加できることをメーカーのアプリで検証できるようにする必要があります。

HomeKitカメラのセキュリティ

IPアドレス（Internet Protocolアドレス）を持つHomeKit対応の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/iPadOS/tvOS/macOSデバイスに直接送信します。ストリームはデバイスおよびIPカメラ（Internet Protocol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。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、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アプリ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。その結果、アプリ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アプリから取得することも許可されません。

HomeKitの安全なビデオ

HomeKitには、Appleや他社にビデオコンテンツを開示することなく、HomeKit対応IPカメラのクリップを記録、解析、表示するための、安全かつ非公開のエンドツーエンドのメカニズムがあります。IPカメラで動きが検知されると、ホームハブとIPカメラ間の専用ローカルネットワーク接続を通じて、ホームハブとして機能しているAppleデバイスにビデオクリップが直接送信されます。このローカルネットワーク接続は、HKDF-SHA512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、ホームハブとIPカメラ間で確立されたHomeKitセッションでネゴシエートされます。HomeKitでは、ホームハブ上でオーディオストリームとビデオストリームを復号し、ビデオフレームをローカルで解析して、重大なイベントがないか確認します。重大なイベントが検出された場合は、ランダムに生成されるAES256鍵を使用してAES-256-GCMでビデオクリップを暗号化します。また、各クリップのポスターフレームも生成します。生成されたポスターフレームは、同じAES256鍵を使用して暗号化されます。暗号化されたポスターフレームとオーディオ/ビデオデータは、iCloudサーバにアップロードされます。暗号鍵を含む各クリップの関連メタデータは、iCloudのエンドツーエンドの暗号化を使用してCloudKitにアップロードされます。

顔の分類のために、HomeKitは使用したデータをすべて保存し、iCloudのエンドツーエンドの暗号化を使用して特定の人の顔をCloudKitで分類します。保存されるデータには、名前やその人の顔を表す画像などの各個人に関する情報が含まれます。これらの顔の画像は、ユーザがオプトインした場合はユーザの「写真」から取得される場合があります。また、以前に分析されたIPカメラのビデオから収集される場合もあります。HomeKit Secure Videoの分析セッションは、この分類データを使用してIPカメラから直接受け取ったセキュアビデオストリーム内の顔を識別し、その識別情報を前述のクリップメタデータに含めます。

ホームアプリを使用してカメラのクリップを表示するときは、iCloudからデータがダウンロードされ、ストリームを復号するための鍵がiCloudのエンドツーエンドの暗号化を使用してローカルでアンラップされます。暗号化されたビデオコンテンツがサーバからストリーミングされ、iOSデバイス上でローカルに復号されてからビューアに表示されます。各ビデオクリップセッションは多くの場合、サブセクションに分解され、各サブセクションではそれぞれの一意の鍵でコンテンツストリームが暗号化されます。

Apple TVでのHomeKitのセキュリティ

HomeKitは他社製の一部のリモコンアクセサリをApple TVに安全に接続し、ホームにあるApple TVのオーナーへのユーザプロファイルの追加をサポートしています。

Apple TVで他社製のリモコンアクセサリを使用する

他社製のHomeKit対応リモコンアクセサリの一部は、ホームアプリを使用して追加され関連付けられたApple TVにヒューマンインターフェイスデザイン(HID)イベントとSiriオーディオを提供します。リモコンからは、HIDイベントが安全なセッションを開始してApple TVに送信されます。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。リモコンからは、専用ローカルネットワーク接続を使用してオーディオフレームがApple TVに直接送信されます。HKDF-SHA512から導出されるセッションごとの鍵ペアは、Apple TVとテレビリモコン間でHomeKitセッションでネゴシエートされ、ローカルネットワーク接続を暗号化するために使用されます。オーディオフレームはApple TV上で復号されてからSiriアプリに転送され、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。

HomeKitホームのApple TVプロファイル

HomeKitホームのユーザがホームにあるApple TVの所有者に自身のプロファイルを追加すると、このユーザは自身のテレビ番組、音楽、ポッドキャストにアクセスできるようになります。Apple TVでの各ユーザのプロファイルの使用に関する設定は、iCloudのエンドツーエンドの暗号化を使用して所有者のiCloudアカウントに送信されます。このデータは各ユーザによって所有され、読み出し専用として所有者に送信されます。ホームの各ユーザは、ホームアプリで、または設定が使用されている所有者のApple TVで、設定値を変更できます。

設定をオンにすると、Apple TVでユーザのiTunesアカウントを利用できるようになります。設定をオフにすると、Apple TVからそのユーザに関するすべてのアカウントとデータが削除されます。CloudKitの最初の共有はユーザのデバイスによって開始され、CloudKitの安全な共有を確立するためのトークンは、ホームのユーザ間でのデータ同期に使用されているものと同じ安全なチャネルを通じて送られます。

iOS、iPadOS、watchOS用のSiriKitのセキュリティ

Siriはアプリの機能拡張システムを使用して他社製アプリと通信します。デバイスでは、Siriはユーザの連絡先情報とデバイスの現在地にアクセスできます。ただし、保護されたデータをアプリに提供するときは、Siriはまずユーザが管理しているアプリのアクセス権を調べます。こうしたアクセス権に応じて、Siriは、ユーザによる元の音声からの関連部分のみをアプリの機能拡張に渡します。例えば、アプリには連絡先情報へのアクセス権がない場合、Siriは「支払いアプリ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係性を解決しません。つまりこの場合、アプリは、「お母さん」という言葉のみ認識します。

一方、ユーザがアプリに連絡先情報へのアクセスを許可している場合、アプリはユーザの母親に関する解決された情報を受け取ります。また、「兄さんはすごい、とメッセージアプリでお母さんに伝えて」など、関係性がメッセージの本文部分で言及されている場合、Siriはアプリのアクセス権に関係なく「兄さん」という言葉の関係性を解決しません。

SiriKit対応アプリは、ユーザの連絡先に登録されている人の名前など、アプリ固有またはユーザ固有の言葉をアプリからSiriに送信できます。この情報によって、Siriの音声認識と自然言語理解でそのアプリの言葉が認識されるようになります。この情報はランダムな識別情報に関連付けられます。こうしたカスタムな情報は、識別情報が使用されている限り使用し続けることができます。ユーザが「設定」でアプリのSiriへの統合を無効にしたり、SiriKit対応アプリがアンインストールされたりすると使用できなくなります。

「RideShareアプリでお母さんの家まで配車を手配して」といったリクエストでは、ユーザの連絡先からの位置データが必要とされます。こうした場合、そのリクエストにおいてのみ、位置情報や連絡先へのそのアプリのアクセス権の設定内容にかかわらず、必要な情報がSiriからアプリの機能拡張に提供されます。

WidgetKitのセキュリティ

WidgetKitは、デベロッパがウィジェットとWatchコンプリケーションを提供するために使用するフレームワークです。どちらにも機密情報が表示されることがあり、「常にオン」画面があるデバイスでは特に、非常に目に付きやすくなる可能性があります。

iOSでは、ロック画面上と「常にオン」のときに機密データを表示するかどうかを、ユーザが構成できます。「設定」では、「設定」>「Face IDとパスコード」の「ロック中にアクセスを許可」セクションで、ロック画面ウィジェットのデータアクセスを無効にすることができます。

Apple Watchでは、「設定」>「画面表示と明るさ」>「常にオン」>「機密コンプリケーションを非表示」と選択することで、「常にオン」のときに機密データを表示するかどうかをユーザが構成できます。また、すべてのコンプリケーションまたは個々のコンプリケーションに墨消し済みの内容を表示することを選択することもできます。

ユーザが個人情報と見なされる内容を非表示にすることを選択した場合、WidgetKitはプレースホルダまたは墨消しをレンダリングします。墨消しを構成するには、デベロッパは次のことを実行する必要があります:

1. `redacted(reason:)`コールバックを実装します。
2. `privacy`プロパティを読み出します。
3. カスタムプレースホルダビューを提供します。

また、デベロッパは`unredacted()`ビュー修飾子を使用してビューを墨消しなしとしてレンダリングすることもできます。

デベロッパは、個々のビューをプライバシーセンシティブとしてマークする代わりに、例えばウィジェットの内容全体がプライバシーセンシティブである場合は、ウィジェット機能拡張にデータ保護機能を追加することができます。ユーザがデバイスのロックを解除して、選択されているプライバシーレベルを照合するまで、WidgetKitにはウィジェットの内容ではなくプレースホルダが表示されます。デベロッパは、Xcodeでウィジェット機能拡張のデータ保護機能を有効にしてから、提供したいプライバシーのレベルに合う値に`Data Protection`エンタイトルメントを設定する必要があります:

- `NSFileProtectionComplete`
- `NSFileProtectionCompleteUnlessOpen`

デバイスがパスコードで保護されている場合、WidgetKitはこれらのウィジェットのコンテンツを非表示にし、デバイスが再起動されてからユーザが認証されるまで、プレースホルダを表示します。また、これらのiOSウィジェットをMacでiPhoneウィジェットとして使用することはできません。

macOS用のDriverKitのセキュリティ

DriverKitは、ユーザが各自のMacにインストールするデバイスドライバをデベロッパが作成できるようにするフレームワークです。DriverKitで作成したドライバは、カーネル拡張機能として実行されるのではなくユーザ空間で実行されるので、システムのセキュリティと安定性が向上します。これによってインストールが簡単になると共に、macOSの安定性とセキュリティが向上します。

ユーザがアプリをダウンロードするだけで（システム機能拡張またはDriverKitを使用する際にはインストーラは不要）、機能拡張が必要な場合にのみ有効になります。kextが使用されている場合、こうした多くのケースで置き換わりますが、/System/Libraryまたは/Libraryへのインストールには管理者権限が必要です。

カーネル拡張機能を必要とするデバイスドライバ、クラウドストレージソリューション、ネットワーク、およびセキュリティアプリを使用するIT管理者の方には、システム機能拡張に基づく新しいバージョンへの移行をおすすめします。新しいバージョンによって、Macでのカーネルパニックのリスクが大きく減少するほか、攻撃領域が狭まります。こうした新しい機能拡張はユーザ空間で実行され、インストールの際に特別な権限を必要としません。また、搭載しているアプリをゴミ箱に移動すると自動的に削除されます。

DriverKitフレームワークは、I/Oサービス、デバイスマッチング、メモリ記述子、ディスパッチキューのためのC++クラスを提供します。また、数字、コレクション、文字列などの一般的な型について、I/Oに適した型の定義も行います。ユーザはUSBDriverKitやHIDDriverKitなどのファミリー固有のドライバフレームワークと共にこれらを使用します。ドライバのインストールとアップグレードにはシステム機能拡張フレームワークを使用してください。

iOSおよびiPadOSでのReplayKitのセキュリティ

ReplayKitはデベロッパが収録やライブブロードキャスト機能をアプリに追加することを可能に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、収録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、アプリプロセスごとに1回表示され、アプリ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アプリのプロセス内ではなく、ReplayKitのデーモンreplayd内で実行されます。これは、収録されたコンテンツがアプリプロセスからはアクセスできないことを保証するためです。
- アプリ内の画面および音声の取り込み: アプリにビデオおよびサンプルのバッファを設けることができます。これは許可を求めるダイアログで保護されています。
- 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、アプリからはアクセスできません。これにより、収録された内容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できます。
- 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ユーザインターフェイスを使用してムービーをプレビューおよび共有できます。このユーザインターフェイスは、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。

ReplayKitによるブロードキャスト

ムービーのブロードキャスト機能には、何層ものセキュリティ機能が埋め込まれています:

- 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ユーザインターフェイス機能拡張
    - 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

このアーキテクチャにより、ブロードキャストされるビデオと音声のコンテンツに関するいかなる権限もホストアプリが持たないことを保証できます。ReplayKitと他社製のブロードキャスト機能拡張のみがアクセスできます。

- ブロードキャストピッカー: ブロードキャストピッカーを使用すると、ユーザは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ユーザインターフェイスを使用して、アプリ内から直接、システムブロードキャストを開始できます。このユーザインターフェイスはプライベートAPI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。これはホスト側アプリとは別のプロセスで実行されます。
- 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機能拡張では、エンコードされていない生のサンプルバッファが使用されます。この処理モードでは、ビデオおよび音声データはシリアル化され、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。

iOSおよびiPadOSでのARKitのセキュリティ

ARKitはデベロッパがアプリやゲームで拡張現実体験を生み出すことを可能にするフレームワークです。デベロッパはiOSまたはiPadOSデバイスの前面カメラまたは背面カメラを使用して、2Dまたは3Dの要素を追加できます。

Appleのカメラはプライバシーを念頭に置いて設計されています。このため、他社製アプリがカメラにアクセスするにはユーザの同意を得る必要があります。iOSおよびiPadOSでは、ユーザがアプリにカメラへのアクセスを許可した場合、そのアプリは前面カメラと背面カメラからのリアルタイムの映像にアクセスできます。カメラを使用中であることが明確でないアプリはカメラを使用できません。

カメラで撮影した写真とビデオには、撮影の場所や日時、被写界深度、オーバーキャプチャなどの情報も含まれていることがあります。カメラアプリで撮影した写真やビデオに位置情報を含めたくない場合、ユーザは「設定」>「プライバシー」>「位置情報サービス」>「カメラ」でいつでも設定を変更できます。写真やビデオを共有するときに場所を含めたくない場合、ユーザは共有シートの「オプション」メニューで位置情報をオフにすることができます。

ユーザのAR体験を向上させるため、ARKitを使用しているアプリは、ほかのカメラからのワールドトラッキング情報またはフェイストラッキング情報を使用できます。ワールドトラッキングでは、ユーザのデバイスのアルゴリズムを使用してこれらのセンサーからの情報を処理し、物理空間との対応関係を確立します。ワールドトラッキングによって「マップ」の光学的方向検知などの機能を実現します。

安全なデバイス管理

安全なデバイス管理の概要

iOS、iPadOS、macOS、tvOS、およびwatchOS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に対応しています。これにより、BYOD（Bring Your Own Device）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、MDMソリューションによって実装されたモバイルデバイス管理（MDM）フレームワークを使用して、パスコード要件の適用、設定の構成、機能の制限を行うことができ、管理対象デバイス上の企業データをリモートでワイプすることもできます。これにより、社員が個人のデバイスを使用して企業データにアクセスするときでも、企業データを保護することができます。

iPhoneおよびiPad用のペアリングモデルのセキュリティ

iOSおよびiPadOS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およびiPadOS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以降、サービスは以下のように動作します。

- 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
- 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
- 写真の同期などの一部のサービスを開始するには、デバイスのロックを解除する必要があります

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 9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、ホストとデバイスで2048ビットのRSA公開鍵が交換されて保存されます。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。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またはFinder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。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、デバイスをホストからWi-Fi経由で接続する必要があるため、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。

com.apple.mobile.pcapdなどの特定の診断サービスは、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とのペアリング関係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。

モバイルデバイス管理

モバイルデバイス管理のセキュリティの概要

Appleのオペレーティングシステムはモバイルデバイス管理（MDM）に対応しています。これによって、組織は規模に応じて導入されているAppleデバイスを安全に設定し、管理することができます。

MDMが安全に機能する仕組み

MDMの機能は、構成、ワイヤレスでの登録、Appleプッシュ通知サービス（APNs）などのオペレーティングシステムのテクノロジーを基礎としています。例えば、APNsは、デバイスをスリープ解除して、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することをトリガするために使用されます。機密情報や専有情報がAPNsを介して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、企業や教育機関の環境へのAppleデバイスの登録、ワイヤレスでの設定の構成やアップデート、準拠状況の監視、ソフトウェアアップデートの管理、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。

iOS 13以降、iPadOS 13.1以降、およびmacOS 10.15以降を搭載したAppleデバイスは、BYOD（Bring Your Own Device）プログラム向けに特別に設計された新しい登録オプションに対応しています。ユーザ登録によって、ユーザは各自の所有デバイスをより自律的に使用できるようになります。一方で企業データは、管理対象のデータを暗号化によって隔離することで、セキュリティが向上します。これによって、BYODプログラムのセキュリティ、プライバシー、ユーザ体験がすべてバランスよく実現します。iOS 17以降、iPadOS 17以降、およびmacOS 14以降では、アカウント駆動型デバイス登録用に同様のデータ隔離メカニズムが追加されています。

登録の種類

- ユーザ登録: ユーザ登録は、ユーザ自身の所有デバイス向けに設計されており、管理対象Apple IDに統合されて、デバイスにユーザの識別情報を確立します。管理対象Apple IDは登録を開始するために必要です。ユーザが登録に成功するには、認証を成功させる必要があります。管理対象Apple IDはユーザがすでにサインインに使用している個人のApple IDと併用できます。管理対象のアプリとアカウントは管理対象Apple IDを使用し、個人用のアプリとアカウントは個人のApple IDを使用します。
- デバイス登録: デバイス登録では、組織がユーザにデバイスを手動で登録させることで、デバイスの使用をさまざまな面にわたって管理できるようになります。これにはユーザがデバイスを消去できるかどうかということも含まれます。デバイス登録には、デバイスに適用できる構成と制限が多数そろっています。ユーザが登録プロファイルを削除すると、すべての構成、設定、およびその登録プロファイルに基づく管理対象アプリが削除されます。ユーザ登録と同様に、デバイス登録も管理対象Apple IDで統合できます。このアカウント駆動型デバイス登録は、個人のApple IDに加えて管理対象Apple IDを使用でき、暗号化によって企業データを隔離します。
- 自動デバイス登録: 自動デバイス登録では、組織はデバイスを入手後すぐに設定し管理することができます。これらのデバイスは**監視対象**と呼ばれ、ユーザがMDMプロファイルを削除するのを防ぐオプションがあります。自動デバイス登録は組織の所有デバイス用に設計されています。

デバイスの機能制限

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、MDMソリューションに登録されている特定のアプリ、サービス、あるいはiPhone、iPad、Mac、Apple TV、またはApple Watch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、構成の一部である機能制限ペイロードとしてデバイスに送信されます。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。

パスコードとパスワードの設定の管理

デフォルトでは、ユーザのパスコードはiOS、iPadOS、およびwatchOSでは数字のPINとして定義できます。Face IDまたはTouch IDを搭載したiPhoneおよびiPadデバイスの場合、デフォルトのパスコードの長さは6桁で、最小長は4桁です。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を使用して、またはiOSとiPadOSでは、Microsoft Exchangeを使用して、複雑なパスコードの要件などのポリシーを適用できます。macOSのパスコードポリシーペイロードを手動でインストールするには管理者パスワードが必要です。パスコードポリシーは、特定のパスコードの長さ、構成、またはその他の属性が必要になる場合があります。

Apple Watchはデフォルトでは数字のパスコードを使用します。管理対象Apple Watchに適用されたパスコードポリシーによって数字以外の文字を使用する必要がある場合は、ペアリングされたiPhoneを使用してデバイスのロックを解除する必要があります。

構成の適用

構成は、MDMソリューションが管理対象デバイスに対してポリシーや制限を適用して管理するための主要な方法です。多数のデバイスを構成したり、多数のデバイスに多くのカスタムのメール設定、ネットワーク設定、または証明書を提供したりする必要がある組織では、構成を使えば、これらを安全かつ確実に行うことができます。

構成

構成とは、XMLプロファイル、または特定の構造に従うjsonフォーマットのファイルで、設定と承認情報をAppleデバイスに読み込むペイロードから成ります。構成は設定、アカウント、制限、資格情報を自動的に構成します。これらのファイルはMDMソリューションまたはMac用Apple Configuratorで作成できます。手動で作成することもできます。組織がAppleデバイスに構成を送信する前に、登録プロファイルを使用してデバイスをMDMソリューションに登録する必要があります。

注記: Mac用Apple Configuratorは、iPhone、iPad、およびApple TVデバイスの構成プロファイルを管理するためにのみ使用できます。

登録プロファイル

登録プロファイルは、デバイスをそのデバイス用に指定されたMDMソリューションに登録する、MDMペイロードを含む構成です。これによってMDMソリューションはコマンドと構成をデバイスに送り、デバイスのいくつかの面を照会することができます。ユーザが登録プロファイルを削除すると、すべての構成、それらの設定、および登録タイプと使用される構成によってはその登録プロファイルに基づく管理対象アプリも、同時に削除されます。1つのデバイスには、同時に1つの登録プロファイルしか存在できません。

構成例

構成には、特定のペイロードに関する次のような多数の設定項目があります（ここに挙げられていない設定項目もあります）：

- パスコードおよびパスワードポリシー
- デバイスの機能制限（カメラを無効にするなど）
- ネットワークとVPNの設定
- Microsoft Exchangeの設定
- メールの設定
- アカウント設定
- 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
- 資格情報と本人確認
- 証明書
- ソフトウェアアップデート

プロファイルの署名と暗号化

構成プロファイルは、署名によって提供元を検証でき、暗号化によって整合性の確保とコンテンツの保護ができます。iOSおよびiPadOSの構成プロファイルはRFC 5652で定められているCMS（Cryptographic Message Syntax）を使用して暗号化されます。CMSは3DESとAES128をサポートします。

プロファイルのインストール

構成は、MDMソリューションを使用して、またはユーザが手動で、デバイスにインストールできます。また、Mac用Apple Configuratorを使用して、iOS、iPadOS、およびtvOSデバイスに構成を導入することもできます。構成によっては、MDMソリューションを使用してインストールする必要があります。プロファイルを削除する方法について詳しくは、「Appleプラットフォーム導入」の「モバイルデバイス管理の概要」を参照してください。

注記: 監視対象のデバイスでは、構成プロファイルをデバイスにロックできます。これは、削除を完全に防止したり、パスコードを入力した場合のみ削除可能にしたりするためです。

自動デバイス登録

組織はデバイスをユーザに渡す前に、デバイスに触れたりデバイスを準備したりすることなく、iOS、iPadOS、macOS、およびtvOSデバイスをモバイルデバイス管理(MDM)ソリューションに自動的に登録できます。Apple School Manager、Apple Business Manager、またはApple Business Essentialsのいずれかのサービスに登録したあと、管理者はサービスWebサイトにサインインし、サービスを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。デバイス構成プロセス時に、デバイスは割り当てられているMDMについてAppleサーバを照会します。割り当てられている場合は、MDMソリューションにアクセスして登録を実行します。自動デバイス登録と互換性のあるMDMソリューションによって、組織は以下のセキュリティ対策を実施できます:

- 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た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。
- 登録の前に、デバイスが最小バージョンのオペレーティングシステムを搭載していることを要求する。
- MacコンピュータでFileVaultの有効化を適用する。

デバイスがMDMに登録されると、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。手順がスキップされていても、より多くのプライバシー保護設定が使用されます。例えば、位置情報サービスを構成するパネルがスキップされても、設定アシスタントでこのサービスは有効化されません。

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、デバイスのライフサイクル全体を通じて構成と制限を設定しておくこともできます。

Apple School Manager、Apple Business Manager、およびApple Business Essentials

Apple School Manager、Apple Business Manager、およびApple Business Essentials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Appleデバイスを導入するためのIT管理者向けサービスです。

MDMソリューションで使用することで、管理者は、これら3つのサービスでユーザの設定プロセスを簡素化したり、デバイス設定を構成したり、購入したアプリやブックを配付したりできます。また、Apple School Managerは直接またはSFTPを使用してStudent Information System(SIS)とも統合されます。3つのサービスはすべてディレクトリ同期とフェデレーション認証に対応しているため、アカウントは組織のIDプロバイダ(IdP)に基づいて自動的にプロビジョニング、アップデート、およびプロビジョニング解除できます。

AppleはISO/IEC 27001や27018の規格に準拠し、認証を取得および維持しているため、Apple製品をご利用のお客様は法令上および契約上の義務を順守できます。こうした認証を取得しているため、お客様にとっては、サポート対象のシステムに対するAppleの情報プライバシーとセキュリティの実践が自ずと証明されることになります。詳しくは、「Appleプラットフォームの認証」の「Appleのインターネットサービスのセキュリティ認証」を参照してください。

注記: 特定の国または地域でAppleのプログラムを利用できるかどうかを確認するには、Appleサポートの記事「教育機関および法人向けのAppleのプログラムやお支払い方法の対応状況」を参照してください。

デバイスの監視

監視対象であるということは一般に、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をより厳密に制御できます。詳しくは、「Appleプラットフォーム導入」の「Appleデバイスの監視について」を参照してください。

監視は、自動デバイス登録の使用時にデバイスで自動的に有効になります。

アクティベーションロックのセキュリティ

Appleがアクティベーションロックを適用する方法は、そのデバイスがiPhoneまたはiPadなのか、Appleシリコン搭載Macなのか、あるいはIntelプロセッサおよびApple T2セキュリティチップ搭載Macなのかによって異なります。

iPhoneとiPadでの動作

iPhoneおよびiPadデバイスでは、アクティベーションロックは、iOSおよびiPadOSの設定アシスタントのWi-Fi選択画面後のアクティベーションプロセスを通じて適用されます。デバイスにアクティベーション中であることが表示されると、アクティベーション証明書を入手するためのリクエストがAppleサーバに送信されます。アクティベーションロックされたデバイスは、この時点でアクティベーションロックを有効にしたユーザのiCloud資格情報を入力するようユーザに求めます。iOSおよびiPadOSの設定アシスタントは、有効な証明書を入手できない限り続行されません。

Appleシリコン搭載Macでの動作

Appleシリコン搭載Macでは、LLBが、デバイスの有効なLocalPolicyが存在することと、LocalPolicyポリシーアンチリプレイ値がセキュアストレージコンポーネントに格納されている値と一致することを確認します。以下の場合には、Low-Level Bootloader（LLB）はrecoveryOSでブートされます:

- 現在のmacOS用のLocalPolicyがない
- LocalPolicyがそのmacOSに対して無効である
- LocalPolicyアンチリプレイ値ハッシュ値がセキュアストレージコンポーネントに格納されている値のハッシュと一致しない

recoveryOSは、Macコンピュータがアクティベートされていないことを検出し、アクティベーションサーバに連絡してアクティベーション証明書を入手します。デバイスがアクティベーションロックされている場合、recoveryOSは、この時点でアクティベーションロックを有効にしたユーザのiCloud資格情報を入力するようユーザに求めます。有効なアクティベーション証明書が入手されると、そのアクティベーション証明書キーがRemotePolicy証明書の入手に使用されます。Macコンピュータは、LocalPolicyキーとRemotePolicy証明書を使用して、有効なLocalPolicyを生成します。LLBは、有効なLocalPolicyが存在しない限り、macOSのブートを許可しません。

Intelプロセッサ搭載Macコンピュータでの動作

IntelプロセッサとT2チップを搭載したMacでは、T2チップのファームウェアが有効なアクティベーション証明書が存在することを確認したあと、コンピュータがmacOSをブートすることを許可します。T2チップによって読み込まれるUEFIファームウェアは、T2チップからデバイスのアクティベーション状況を照会し、有効なアクティベーション証明書が存在しない場合はmacOSをブートする代わりにrecoveryOSをブートします。recoveryOSはMacがアクティベートされていないことを検出し、アクティベーションサーバに連絡してアクティベーション証明書を入手します。デバイスがアクティベーションロックされている場合、recoveryOSは、この時点でアクティベーションロックを有効にしたユーザのiCloud資格情報を入力するようユーザに求めます。UEFIファームウェアは、有効なアクティベーション証明書が存在しない限り、macOSのブートを許可しません。

管理対象紛失モードとリモートワイプ

管理対象紛失モードは、監視対象のデバイスが盗難に遭った際にそのデバイスを見つけるために使用されます。見つかったら、リモートでロックまたは消去することができます。

管理対象紛失モード

iOS 9以降を搭載した監視対象のiOSまたはiPadOSデバイスの紛失や盗難の際には、モバイルデバイス管理（MDM）の管理者はそのデバイスの紛失モード（「管理対象紛失モード」と呼ばれます）をリモートで有効にすることができます。管理対象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。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することもできます（位置情報サービスがオフになっている場合でも）。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。管理者が管理対象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。

リモートワイプ

iPhone、iPad、Mac、Apple TV、およびApple Watchデバイスは、管理者またはユーザがリモートで消去して、すべてのデータを読み取り不能にできます。

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MDMソリューションに確認応答を送り返し、ワイプを実行します。Microsoft Exchange ActiveSyncによるリモートワイプの場合は、デバイスがMicrosoft Exchange Serverにチェックインしてから、ワイプを実行します。

以下の状況ではリモートワイプを実行できません:

- ユーザ登録が使用されている
- ユーザ登録でアカウントをインストールしたときにMicrosoft Exchange ActiveSyncが使用されている
- デバイスが監視されている場合にMicrosoft Exchange ActiveSyncが使用されている

ユーザは自分が所有する対応デバイスを、「設定」（iPhoneおよびiPad）または「システム設定」（Mac）を使用してワイプすることもできます。前に述べたようにパスコードの誤入力が続いた場合にiPhone、iPad、およびApple Watch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。

AppleシリコンMacコンピュータとApple T2セキュリティチップを搭載したMacコンピュータでは、またはFileVaultがオンになっている場合は、リモートワイプを瞬時に実行できます。メディア鍵を安全に破棄することによって、リモートワイプを瞬時に実行できます。

iPadOSの共有iPadのセキュリティ

共有iPadとは、iPadの導入で使用するマルチユーザモード構成のiPadのことです。ユーザは、各自の書類やデータが分離された状態を保ちながら1台のiPadを共有できます。ユーザにはそれぞれ、個人用の予約済み保存領域が割り当てられます。この領域は、ユーザの資格情報で保護されたAPFS（Apple File System）ボリュームとして実装されます。共有iPadでは、組織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は複数のユーザで使用できるように構成されているため、ユーザは組織が所有するどのiPadにもサインインできます。ユーザのデータは、それぞれのデータ保護ドメイン内の個別の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。iPadOS 13.4以降では、ユーザは一時セッションにサインインすることもできます。ユーザが一時セッションからサインアウトすると、ユーザのAPFSボリュームが削除され、予約済みの領域はシステムに戻されます。

共有iPadへのサインイン

共有iPadへのサインインには、既存の管理対象Apple IDと、連携された管理対象Apple IDの両方を使用できます。連携されたアカウントを初めて使用する際には、ユーザはアイデンティティプロバイダ（IdP）のサインインポータルにリダイレクトされます。認証後に、背後にある管理対象Apple ID用の一時的なアクセストークンが発行されます。ログインプロセスは既存の管理対象Apple IDでのサインインプロセスと同様に進行します。サインインすると、共有iPadの設定アシスタントによって、ユーザはパスコード（資格情報）の設定を求められます。このパスコードは、今後デバイス上のローカルデータの保護とログイン画面の認証に使用されることになります。単一ユーザのデバイスでは、ユーザは連携された自身のアカウントを使用して管理対象Apple IDに1回サインインすれば、そのあとはパスコードで各自のデバイスのロックを解除します。これと同様に、共有iPadでは、ユーザは連携された自身のアカウントを使用して1回サインインしたあと、以降は設定したパスコードを使用します。

ユーザがフェデレーション認証での認証を行わずにサインインすると、管理対象Apple IDがApple Identity Service（IDS）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。ユーザ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。

ユーザがそのデバイスを以前に使ったことがない場合、または一時セッション機能を使用している場合は、共有iPadによって新しいUNIXユーザID、ユーザの個人用データを保存するAPFSボリューム、およびローカルキーチェーンがプロビジョニングされます。保存領域はAPFSボリュームの作成時にユーザに割り当てられる（予約される）ため、新しいボリュームを作成するための容量が不足する場合があります。そのような場合は、クラウドへのデータの同期が完了した既存ユーザが特定され、新しいユーザがサインインできるように、そのユーザがデバイスから排除されます。すべての既存ユーザがクラウドデータのアップロードを完了していない場合、新しいユーザはサインインできません。新しいユーザがサインインするには、1人のユーザのデータの同期が終了するまで待つ必要があります。または、管理者に既存ユーザのアカウントを強制的に削除してもらうこともできますが、その場合はデータが損失するおそれがあります。

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（ユーザが利用できるWi-Fiアクセスポイントがない場合など）、特定の日数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または一時セッション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。

ユーザ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、ユーザの設定が復元され、その生徒の書類やデータがiCloudから同期されます。

ユーザ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、ユーザのサインアウト後も変更内容がiCloudに、またはNSURLSessionバックグラウンドセッションを使用してその他のWebサービス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ます。ユーザがサインインし直すまで再度マウントすることはできません。

一時セッションのデータはiCloudに同期されません。また、一時セッションでBoxやGoogle Driveなどの他社の同期サービスにサインインすることはできますが、一時セッションが終了した際にデータの同期を継続する仕組みはありません。

共有iPadからのサインアウト

ユーザが共有iPadからサインアウトすると、そのユーザのキーバッグがただちにロックされ、すべてのアプリが終了されます。このとき、次に使うユーザが素早くサインインできるように、iPadOSでは通常のサインアウト処理の一部が一時保留になり、次のユーザ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）内にユーザがサインインした場合は、新しいユーザアカウントへ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起動します。

一時セッションが終了すると、共有iPadで完全なログアウトシーケンスが実行され、一時セッションのAPFSボリュームがただちに削除されます。

Apple Configuratorのセキュリティ

Mac用Apple Configuratorは、柔軟で安全、デバイス中心の設計を特徴としており、管理者はUSB経由でMacに接続されている1台または数十台のiOS、iPadOS、およびtvOSデバイス（またはBonjourを通じてペアリングされたtvOSデバイス）をユーザに配付する前に素早く簡単に構成できます。Mac用Apple Configuratorでは、管理者はソフトウェアをアップデートしたり、アプリや構成プロファイルをインストールしたり、デバイスの壁紙または壁紙の名前を変更したり、デバイスの情報や書類を書き出したりするなど、多くのことができます。

また、Mac用Apple Configuratorでは、AppleシリコンまたはApple T2セキュリティチップを搭載したMacコンピュータを復活させるまたは復元することもできます。この方法でMacを復活させるまたは復元すると、オペレーティングシステム（macOS、Appleシリコンの場合はrecoveryOS、T2の場合はsepOS）の最新のマイナーアップデートを含むファイルがAppleのサーバから安全にダウンロードされ、Macに直接インストールされます。復活または復元に成功すると、ファイルはApple Configuratorを実行しているMacから削除されます。いかなる場合にも、このファイルをユーザがApple Configuratorの外部で調査したり使用したりすることはできません。

管理者はMac用Apple ConfiguratorまたはiPhone用Apple Configuratorを使用して、デバイスをApple School Manager、Apple Business Manager、またはApple Business Essentialsに追加することもできます。AppleまたはApple正規取扱店か正規通信事業者から直接購入していないデバイスでも問題ありません。手動で登録されたデバイスを管理者が設定すると、そのデバイスは強制的に監視対象になりモバイルデバイス管理（MDM）に登録され、それらのサービスの1つに登録されたその他のデバイスと同様に動作します。直接購入ではないデバイスの場合、試用期間として30日間、ユーザはそれらのサービスの1つ、監視、およびMDMからデバイスを解除できます。

また、iOS、iPadOS、およびtvOSデバイスにインターネット接続がまったくない場合は、デバイスの設定中にインターネット接続のあるホストMacに接続することで、組織がMac用Apple Configuratorを使用してデバイスをアクティベートすることができます。管理者はWi-Fiやモバイルデータ通信ネットワークに接続しなくても、アプリ、プロファイル、書類などの必要な構成と共にデバイスを復元、アクティベート、準備することができます。この機能では、テザリングを使用しないアクティベーション中に通常必要とされる既存のアクティベーションロックの要件を管理者がバイパスすることはできません。

スクリーンタイムのセキュリティ

スクリーンタイムは、大人や子供がアプリやWebサイトなどにどれだけ時間を使っているかを確認して管理するために組み込まれている機能です。大人と(管理対象の)子供という2種類のユーザがいます。

スクリーンタイムはシステムセキュリティの新機能というわけではありませんが、デバイス間で収集および共有されているデータのプライバシーとセキュリティをスクリーンタイムが保護する仕組みを理解しておくことは重要です。スクリーンタイムはiOS 12以降、iPadOS 13.1以降、macOS 10.15以降で利用でき、watchOS 6以降の一部の機能でも利用できます。

以下は、スクリーンタイムの主な機能を示した表です。

機能	対応オペレーティングシステム
使用状況を表示する	iOS iPadOS macOS
その他の制限を適用する	iOS iPadOS macOS watchOS
Webの使用制限を設定する	iOS iPadOS macOS
アプリの制限を設定する	iOS iPadOS macOS watchOS
休止時間を設定する	iOS iPadOS macOS watchOS

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ンです)。スクリーンタイムは、以前のバージョンのiOSとiPadOSにあった「機能制限」機能、および以前のバージョンのmacOSにあったペアレンタルコントロール機能に代わる機能です。

iOS 13以降、iPadOS 13.1以降、およびmacOS 10.15以降では、スクリーンタイムのユーザと管理対象の子供のiCloudアカウントで2ファクタ認証が有効になっている場合、各自のデバイス使用状況がデバイス間で自動的に共有されます。ユーザがSafariの履歴を消去したりアプリ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、iPadOS、およびmacOS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。子供は成年（年齢は国や地域によって異なります）に達すると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）プロトコルによるエンドツーエンドの暗号化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読み込まれるまでIDSサーバに一時保存される場合があります（iPhoneまたは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」）
- 制限を設けたあとのカテゴリの使用状況の変化（90日以内）
- 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
- アプリ制限数
- スクリーンタイム設定でユーザが使用状況を閲覧した回数（ユーザの種類および閲覧の種類（ローカル、リモート、ウィジェット）ごと）
- ユーザが制限を無視した回数（ユーザの種類ごと）
- ユーザが制限を削除した回数（ユーザの種類ごと）

アプリや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アプリ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。

用語集

AES-XTS IEEE 1619-2007で規定されているAESのモード。ストレージメディアの暗号化に使用されます。

AES（Advanced Encryption Standard） データを暗号化することで非公開にしておくために使用される、世界的に普及している暗号化規格。

AES暗号化エンジン AESを実装する専用ハードウェアコンポーネント。

APFS（Apple File System） iOS、iPadOS、tvOS、watchOS、およびmacOS 10.13以降を搭載したMacコンピュータのデフォルトのファイルシステム。APFSは強力な暗号化、スペース共有、スナップショット、ディレクトリサイズの高速計算、改良されたファイルシステム基盤を備えています。

Apple Business Manager 組織がAppleまたは提携しているApple正規取扱店や通信事業者から直接購入したAppleデバイスを迅速かつ効率的に導入するための、シンプルなWebベースのIT管理者向けポータル。ユーザに渡す前にデバイスに触れたりデバイスを準備したりしなくても、デバイスをモバイルデバイス管理（MDM）ソリューションに自動的に登録できます。

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 School Manager 組織がAppleまたは提携しているApple正規取扱店や通信事業者から直接購入したAppleデバイスを迅速かつ効率的に導入するための、シンプルなWebベースのIT管理者向けポータル。ユーザに渡す前にデバイスに触れたりデバイスを準備したりしなくても、デバイスをモバイルデバイス管理（MDM）ソリューションに自動的に登録できます。

Appleセキュリティバウンティ 最新リリースのオペレーティングシステム、および該当する場合は最新のハードウェアに影響する脆弱性について情報提供した研究者を対象に、Appleが支払う報奨金。

Appleプッシュ通知サービス（APNs） Apple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。

Boot Camp 対応するMacコンピュータへのMicrosoft Windowsのインストールをサポートするユーティリティ。

Boot ROM デバイスが起動したときにデバイスのプロセッサによって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。

CKRecord CloudKitに保存されるデータ、またはCloudKitから取得されるデータが含まれる、キー値ペアの辞書。

Data Vault リクエスト元のアプリ自体がサンドボックス化されているかどうかに関係なく、データへの不正アクセスから保護するためにカーネルによって適用されるメカニズム。

ECDSA（楕円曲線デジタル署名アルゴリズム） 楕円曲線暗号に基づいた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。

Exclusive Chip Identification（ECID） 各iPhoneおよびiPadのプロセッサに固有の64ビットの識別情報。

Gatekeeper macOSに搭載された、信頼されたソフトウェアのみがユーザのMac上で動作することを保証するために設計されたテクノロジー。

HMAC 暗号学的ハッシュ関数に基づいたハッシュベースのメッセージ認証コード。

iBoot すべてのAppleデバイス用のステージ2ブートローダー。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。System on Chip（SoC）の世代に応じて、Low Level Bootloader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。

Input/Output Memory Management Unit（IOMMU） 入出力メモリ管理装置。他の入出力デバイスや周辺機器からのアドレス空間へのアクセスを制御する集積チップのサブシステムです。

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。

Low-Level Bootloader（LLB） 2ステージの起動アーキテクチャがあるMacコンピュータでは、LLBに含まれるコードがBoot ROMに呼び出され、次にそのコードがセキュアブートチェーンの一部としてiBootを読み込みます。

NAND 不揮発性フラッシュメモリ。

Per Fileキー ファイルシステム上のファイルを暗号化するためにデータ保護で使用されるキー。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。

sepOS AppleがカスタマイズしたL4マイクロカーネルのバージョンに基づいたSecure Enclaveファームウェア。

SSDコントローラ ストレージメディア（ソリッドステートドライブ）を管理するハードウェアサブシステム。

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。

Unified Extensible Firmware Interface（UEFi）ファームウェア BIOSに代わるテクノロジーであり、ファームウェアとコンピュータのオペレーティングシステムをつなぐインターフェイス。

Uniform Resource Identifier（URI） Webベースのリソースを識別する文字列。

xART eXtended Anti-Replay Technologyの略。Secure Enclave用の暗号化された認証済み永続ストレージを提供する一連のサービスのことであり、物理ストレージアーキテクチャに基づくアンチリプレイ機能を備えています。セキュアストレージコンポーネントを参照してください。

XNU Appleの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、アドレス空間配置のランダム化（ASLR）などのセキュリティ対策を実行します。

XProtect macOSに搭載された、署名に基づいたマルウェアの検出と削除が可能なアンチウイルステクノロジー。

アドレス空間配置のランダム化（ASLR） オペレーティングシステムに採用されている、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。

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Appleのオペレーティングシステムおよび他社製アプリで使用されるインフラストラクチャおよびAPIセット。

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 12以降では4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。

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。

シールドキー保護(SKP) システムソフトウェアとハードウェアでのみ利用可能な鍵(Secure EnclaveのUIDなど)の測定によって暗号鍵を保護(または**封印**)するデータ保護のテクノロジー。

システムコプロセッサ整合性保護(SCIP) Appleが使用している、コプロセッサファームウェアの変更を防ぐためのメカニズム。

システムソフトウェア認証 ハードウェアに組み込まれた暗号鍵とオンラインサービスを組み合わせて使用し、サポート対象のデバイスに適した、Appleからの正当なソフトウェアのみがアップグレード時に提供され、インストールされることを保証するプロセス。

セキュアストレージコンポーネント このコンポーネントは、変更不可のRO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。対応デバイスでは、Secure Enclaveはアンチリプレイ値の保存のために、セキュアストレージコンポーネントとペアになっています。アンチリプレイ値を読み取ってアップデートするために、Secure Enclaveとストレージチップは、アンチリプレイ値への独占的アクセスを保証するためのセキュアプロトコルを使用しています。このテクノロジーには複数の世代があり、保証されるセキュリティが異なります。

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とオペレーティングシステムは、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。

ダイレクトメモリアクセス(DMA) ハードウェアサブシステムがCPUをバイパスしてメインメモリに直接アクセスできるようにする機能。

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。このプロセスによって、そのデバイスを侵害するには総当たり(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。

データ保護 サポートされているAppleデバイス用のファイルおよびキーチェーン保護メカニズム。アプリで使用される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)モード 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またはFinderを実行しているコンピュータに接続すると、「Finder(またはiTunes)はリカバリモードの(iPhoneまたはiPad)を見つけました。Finder(またはiTunes)でご利用になる前に、この(iPhoneまたは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。

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。

パスコードから導出された鍵(PDK) ユーザパスワードを長期SKP鍵およびSecure EnclaveのUIDとタングルして導出された暗号鍵。

ファイルシステムキー 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。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。

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(デバイスファームウェアアップデート(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、System on Chip(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。

プロビジョニングプロファイル アプリをiOSまたはiPadOS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(.plistファイル)。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アプリのアプリ IDが含まれます。

メディア鍵 安全で瞬時のワイプを可能にする暗号鍵階層の一部。iOS、iPadOS、tvOS、およびwatchOSでは、メディア鍵によってデータボリューム上のメタデータがラップされます(そのため、この鍵なしですべてのPer Fileキーにアクセスすることは不可能で、データ保護で保護されているファイルはアクセスできなくなります)。macOSでは、メディア鍵によって、FileVaultで保護されたボリューム上の鍵マテリアル、すべてのメタデータ、およびデータがラップされます。いずれの場合も、メディア鍵をワイプすると、暗号化されたデータにアクセスできなくなります。

メモリコントローラ System on Chipとそのメインメモリ間のインターフェイスを制御する、System on Chipのサブシステム。

モバイルデバイス管理(MDM) 登録したデバイスを管理者がリモートで管理できるサービス。デバイスを登録すると、管理者はネットワーク経由でMDMサービスを使用し、ユーザ操作なしで、設定の構成といったさまざまなタスクをデバイスで実行できます。

ユニークID(UID) 製造時に各プロセッサに焼き付けられるAES 256ビットキー。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物理的な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などのほかの識別情報に関連しません。

リカバリモード ユーザのデバイスが認識されない場合に、多くのAppleデバイスを復元するために使用されるモード。オペレーティングシステムを再インストールすることができます。

拡張シリアルペリフェラルインターフェイス(eSPI) 同期式シリアル通信用に設計された一体型バス。

鍵ラッピング 1つの鍵を別の鍵で暗号化すること。iOSおよびiPadOSではRFC 3394準拠のNIST AES鍵ラッピングが使用されます。

集積回路(IC) **マイクロチップ**とも呼ばれます。

楕円曲線Diffie-Hellman一時鍵共有(ECDHE) 楕円曲線に基づいた鍵交換メカニズム。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者が秘密鍵を共有できます。

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。

改訂履歴

改訂履歴

2024年5月

追加されたトピック:

- Cryptex1 Image4マニフェストハッシュ(spih)
- Cryptex1生成(stng)
- 「メッセージ」とIDS用のBlastDoor
- ロックダウンモードのセキュリティ
- App Storeのセキュリティについて
- WidgetKitのセキュリティ

アップデートされたトピック:

- Appleプラットフォームのセキュリティの概要
- Apple SoCのセキュリティ
- Secure Enclave
- Face ID、Touch ID、パスコード、パスワード
- 顔照合のセキュリティ
- Face IDとTouch IDの用途
- 予備電力機能付きエクスプレスカード
- オペレーティングシステムの整合性
- データ接続の安全な有効化
- iPhoneおよびiPad用のアクセサリの検証
- watchOSのシステムのセキュリティ
- パスコードとパスワード
- データ保護の概要
- データ保護用のキーバッグ
- 代替起動モードでの鍵の保護
- 攻撃を受けたときのユーザデータ保護

- macOSでのFileVaultの管理
- iOSおよびiPadOSでのアプリのセキュリティの概要
- macOSでのGatekeeperおよびランタイム保護
- 管理対象Apple IDのセキュリティ
- iCloudの暗号化
- アカウント復旧用連絡先のセキュリティ
- 故人アカウント管理連絡先のセキュリティ
- iCloudキーチェーンのセキュリティの概要
- キーチェーンの安全な同期
- iCloudキーチェーンエスクローのセキュリティ
- カードのプロビジョニングのセキュリティの概要
- 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
- Apple Payを使ってカードで支払う
- Apple Cardのセキュリティ
- 「iPhoneのタッチ決済」のセキュリティ
- Appleウォレットを使用したアクセス
- アクセス鍵のタイプ
- Appleウォレットでの本人確認書類
- Appleウォレットでの本人確認書類のセキュリティ
- デベロッパキットのセキュリティの概要
- HomeKitの通信のセキュリティ
- モバイルデバイス管理のセキュリティの概要
- 構成の適用

2022年12月

追加されたトピック:

- iCloudの高度なデータ保護

アップデートされたトピック:

- iCloudのセキュリティの概要
- iCloudの暗号化
- iCloudバックアップのセキュリティ
- アカウント復旧用連絡先のセキュリティ
- 故人アカウント管理連絡先のセキュリティ

2022年5月

アップデート対象:

- iOS 15.4
- iPadOS 15.4
- macOS 12.3
- tvOS 15.4
- watchOS 8.5

追加されたトピック:

- ペアリングされたrecoveryOSの制限
- ローカルオペレーティングシステムのバージョン(love)
- ヘルスケア共有
- アカウント復旧用連絡先のセキュリティ
- 故人アカウント管理連絡先のセキュリティ
- 「iPhoneのタッチ決済」のセキュリティ
- Appleウォレットを使用したアクセス
- アクセス鍵のタイプ
- Appleウォレットでの本人確認書類
- Siri対応HomeKitアクセサリ

アップデートされたトピック:

- Touch ID搭載Magic Keyboard
- Face ID、Touch ID、パスコード、パスワード
- 顔照合のセキュリティ
- 予備電力機能付きエクスプレスカード
- Appleシリコン搭載Macのブートモード
- AppleシリコンMacのLocalPolicyファイルの内容
- 署名済みシステムボリュームのセキュリティ
- watchOSのシステムのセキュリティ
- Apple Security Research Device
- Apple File Systemの役割
- アプリのユーザデータへのアクセスの保護
- macOSでのアプリのセキュリティの概要
- macOSでのマルウェアからの保護
- iCloudのセキュリティの概要
- キーチェーンの安全な同期
- 安全なiCloudキーチェーン復元
- Apple Payを使ってカードで支払う
- Apple Payの非接触型パス

- カードをApple Payで使用不可にする
- Apple Cardの申し込み
- Apple Cashのセキュリティ
- Appleウォレットに交通系ICカードや電子マネーカードを追加する
- 安全なApple Messages for Business
- FaceTimeのセキュリティ
- iOSでの車のキーのセキュリティ
- Apple Configuratorのセキュリティ

削除されたトピック:

- HomeKit対応アクセサリとiCloud

2021年5月

アップデート対象:

- iOS 14.5
- iPadOS 14.5
- macOS 11.3
- tvOS 14.5
- watchOS 7.4

追加されたトピック:

- Touch ID搭載Magic Keyboard。
- セキュアインテントとSecure Enclaveへの接続。
- 自動ロック解除とApple Watch。
- CustomOS Image4マニフェストハッシュ(coih)。

アップデートされたトピック:

- 予備電力機能付きエクスプレスカードに2つの新しいエクスプレスモードトランザクションを追加。
- Secure Enclave機能の概要をアップデート。
- 安全なマルチブート(smb3)にソフトウェアアップデートに関する内容を追加。
- シールドキー保護(SKP)に内容を追加。

2021年2月

アップデート対象:

- iOS 14.3
- iPadOS 14.3
- macOS 11.1
- tvOS 14.3
- watchOS 7.2

追加されたトピック:

- メモリセーフなiBoot実装
- Appleシリコン搭載Macのブートプロセス
- Appleシリコン搭載Macのブートモード
- Appleシリコン搭載Macの起動ディスクのセキュリティポリシー管理
- LocalPolicyの署名キーの作成と管理
- AppleシリコンMacのLocalPolicyファイルの内容
- 署名済みシステムボリュームのセキュリティ
- Apple Security Research Device
- パスワードの監視
- IPv6のセキュリティ
- iOSでの車のキーのセキュリティ

アップデートされたトピック:

- Secure Enclave
- ハードウェアマイクの切断
- Intelプロセッサ搭載MacのrecoveryOSおよび診断環境
- Macコンピュータでのダイレクトメモリアクセス保護
- macOSのカーネルの安全な拡張
- システム整合性保護
- watchOSのシステムのセキュリティ
- macOSでのFileVaultの管理
- アプリから保存済みパスワードへのアクセス
- パスワードのセキュリティに関する勧告
- Apple Cashのセキュリティ
- 安全なApple Messages for Business
- Wi-Fiのプライバシー
- アクティベーションロックのセキュリティ
- Apple Configuratorのセキュリティ

2020年4月

アップデート対象:

- iOS 13.4
- iPadOS 13.4
- macOS 10.15.4
- tvOS 13.4
- watchOS 6.2

アップデート:

- ハードウェアマイクの切断にiPadのマイク切断を追加。
- アプリのユーザデータへのアクセスの保護にData Vaultを追加。
- macOSでのFileVaultの管理およびコマンドラインツールをアップデート。
- macOSでのマルウェアからの保護に「マルウェア削除ツール」を追加。
- iPadOSの共有iPadのセキュリティをアップデート。

2019年12月

「iOSセキュリティガイド」、「macOSのセキュリティの概要」、「Apple T2セキュリティチップの概要」を統合

アップデート対象:

- iOS 13.3
- iPadOS 13.3
- macOS 10.15.2
- tvOS 13.3
- watchOS 6.1.1

プライバシーの制御、SiriとSiriからの提案、およびSafariのインテリジェントトラッキング防止機能が削除されました。これらの機能の最新情報は、https://www.apple.com/jp/privacy/を参照してください。

2019年5月

iOS 12.3向けにアップデート

- TLS 1.3のサポート
- AirDropのセキュリティに関する説明を改訂
- DFUモードとリカバリモード
- アクセサリの接続のパスコード要件

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
- 予備電力機能付き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からの提案
- Siriのショートカット
- ショートカットアプリ
- 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

2017年10月

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のアップデート
- Apple Pay、Apple PayによるWeb上での支払い
- Siriからの提案
- 共有iPad

2017年7月

iOS 10.3向けにアップデート

- Secure 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

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

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
- 秘密メモ
- Apple School Manager
- 共有iPad

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
- エンタープライズアプリの信頼モデル
- 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アプリ
- 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

著作権

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com
Apple Japan, Inc.
〒106-6140 東京都港区六本木6丁目10番1号 六本木ヒルズ
apple.com/jp

J028-00780