Apple at Work

プラットフォームのセキュリティ

設計時から安全性を考慮。

Appleはセキュリティを重視し、ユーザー保護と企業データ保護の両方に真剣に取り組んでいます。私たちは高度なセキュリティ機能を最初から製品に組み込み、設計時から安全性を考慮してきました。そして、優れたユーザー体験と高度なセキュリティ機能を両立し、ユーザーが望む方法で自由に仕事ができるようにしています。セキュリティに対するこのような包括的なアプローチが可能なのは、ハードウェア、ソフトウェア、サービスを統合した製品を作っているAppleだけです。

ハードウェアのセキュリティ

ソフトウェアのセキュリティを保つには、ハードウェアにセキュリティの基盤を組み込む必要があります。そのため、iOS、iPadOS、macOS、tvOS、watchOSを搭載したAppleデバイスのシリコンには、セキュリティ機能が内蔵されています。

これには、システムのセキュリティ機能を駆動するカスタムCPUやセキュリティ機能専用の追加シリコンが含まれます。セキュリティを重視したハードウェアは、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的な機能をサポートするという原則に従っています。このようなコンポーネントとして、セキュアブートのためにハードウェアの信頼の起点を提供するBoot ROM、効率的かつ安全な暗号化／復号を行う専用のAESエンジン、Secure Enclaveがあります。

Secure Enclaveはシステムオンチップ（SoC）で、iPhone、iPad、Apple Watch、Apple TV、HomePodデバイスのすべての現行モデル、Appleシリコンを搭載したMac、Apple T2セキュリティチップを搭載したMacに搭載されています。SoCの設計原則に従い、Secure Enclaveには専用のBoot ROMとAESエンジンがあります。また、Secure Enclaveは、保存されているデータの暗号化に必要な鍵をセキュアに生成、保管するための基盤を提供し、Touch IDとFace IDの生体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（鍵マテリアル）がさらされることも避けなければなりません。AESハードウェアエンジンは、ファイルの書き込みや読み取り時に高速のインライン暗号化／復号を行うことによってこの問題を解決します。アプリケーションプロセッサ（CPU）やオペレーティングシステム全体に情報が漏れないように、Secure Enclaveから特別なチャネルを通じて、必要な鍵マテリアルをAESエンジンに提供します。これによって、Appleのデータ保護テクノロジーとFileVaultテクノロジーは、存続期間の長い暗号鍵を危険にさらすことなく、ユーザーのファイルを確実に保護できます。

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が改ざんされることを防止し、Appleの信頼できるオペレーティングシステムだけが起動時に読み込まれるようにします。セキュアブートはBoot ROMと呼ばれる変更不可のコードから始まります。Boot ROMはApple SoCの

製造時に書き込まれ、ハードウェアの信頼の起点となります。T2チップを搭載したMacコンピュータでは、T2チップが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の両方とも、それぞれ別のBoot ROMを使った独自のセキュアブートプロセスも実行します。これは、Aシリーズのチップと M1チップがセキュアに起動する方法と同じです）。

Secure Enclaveは、AppleデバイスのTouch IDとFace IDの指紋データおよび顔データも処理します。これにより、ユーザーの生体データのプライバシーとセキュリティを保護しつつ、安全な認証を提供します。これによってユーザーは、アクセスや購入といった多くの状況で、長くて複雑なパスコードやパスワードと同等のセキュリティを、すばやく便利な認証方法で利用できるようになります。

Appleデバイスのこのようなセキュリティ機能は、Apple独自のシリコン設計、ハードウェア、ソフトウェア、サービスの組み合わせによって実現しています。

システムのセキュリティ
システムのセキュリティは、Appleのハードウェアの独自機能を基盤として、使いやすさを損なうことなく、Appleデバイスのシステムリソースに対する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、起動プロセス、ソフトウェアアップデートのほか、CPU、メモリ、ディスク、ソフトウェアプログラム、保存されているデータといったコンピュータシステムリソースの保護にもおよびます。

最新バージョンのAppleオペレーティングシステムは、最も安全です。システムの起動時にマルウェアに感染しないように保護するセキュアブートは、Appleのセキュリティの重要な部分です。セキュアブートはハードウェアから始まり、ソフトウェアを通して信頼チェーンを確立します。それぞれのステップでは、次のステップが適切に機能していることを確認してから制御が引き渡されます。このセキュリティモデルは、Appleのデバイスのデフォルトの起動方法だけではなく、Appleデバイスの復元や適切なタイミングでのアップデートなど、様々なモードもサポートしています。T2チップやSecure Enclaveなどのサブコンポーネントは、独自のセキュアブートを実行して、Appleから提供された動作確認済みのコードだけが起動されるようにしています。アップデートの仕組みはダウングレード攻撃への防御にもなります。デバイスのオペレーティングシステムを、データを盗む目的で（攻撃者が侵入方法を知っている）旧バージョンに戻す（ロールバックする）ことができなくなるからです。

また、Appleのデバイスには起動とランタイムの保護機能が組み込まれているので、実行中もデバイスの整合性が保たれます。iPhone、iPad、Apple Watch、Apple TV、HomePodに搭載されているAppleのシリコンと、Appleシリコンが搭載されたMac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提供します。macOSには、すべてのMacハードウェアプラットフォームでサポートされる機能に加えて、様々なコンピューティングモデルをサポートする、拡張された構成可能な保護機能のセットも搭載されています。

暗号化とデータ保護
Appleのデバイスは暗号化機能でユーザーのデータを保護しています。デバイスの盗難や紛失時には、リモートワイプを行うこともできます。

セキュアブートチェーン、システムセキュリティ、アプリケーションのセキュリティ機能はすべて、信頼されたコードとアプリケーションのみがデバイス上で実行されることを保証するためのものです。Appleのデバイスにはほかにも暗号化の機能が搭載されており、セキュリティインフラの一部が危険にさらされた場合（デバイスの盗難／紛失時や信頼されていないコードの実行時など）でも、ユーザーのデータは保護されます。これにより、個人と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、ユーザーとIT管理者の双方がメリットを得ることができます。

iOSとiPadOS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ベースのMacは、FileVaultと呼ばれるボリューム暗号化テクノロジーでデータを保護します。Appleシリコンが搭載されたMacでは、データ保護をサポートするハイブリッドモデルが

使用されます。ただし、以下の2つの点に注意してください。最小保護レベル（クラスD）はサポートされません。デフォルトレベル（クラスC）ではボリュームキーが使用され、Intelベースの MacのFileVaultと同じように動作します。いずれの場合も、鍵管理階層がSecure Enclaveの専用シリコンにあり、専用のAESエンジンが高速な暗号化をサポートすることで、（危殆化のリスクがある）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ことを保証しています（IntelベースのMacのうち、T1を搭載しているモデル、またはSecure Enclaveを搭載していないモデルでは、FileVaultの暗号鍵を保護する専用シリコンは使用されません）。

Appleは、データ保護やFileVaultを使用してデータへの不正アクセスを防止しているほか、オペレーティングシステムカーネルで保護とセキュリティを強化しています。カーネルは、アプリケーションをサンドボックス化する（アプリケーションがアクセスできるデータを制限する）ためのアクセス制御を実施し、Data Vaultと呼ばれる仕組み（アプリケーションが実行できる呼び出しを制限するのではなく、ほかのすべての要求元アプリケーションからアプリケーションデータへのアクセスを制限する機能）を使用します。

アプリケーションのセキュリティ

アプリケーションは、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。アプリケーションは、仕事を効率化する上で非常に大きなメリットをもたらす一方で、適切に扱わないとシステムのセキュリティ、安定性、ユーザーデータに悪影響を及ぼす可能性があります。

このため、Appleは何層もの保護を構築して、アプリケーションが既知のマルウェアに感染したり改ざんされたりしないよう保護しています。追加の保護機能により、アプリケーションからユーザーデータへのアクセスは慎重に管理されます。このようなセキュリティ管理機能によって安定かつ安全なアプリケーションのプラットフォームが実現しているので、何千ものデベロッパが数十万ものiOS、iPadOS、macOSアプリケーションを提供しても、システムの整合性が損なわれることがありません。また、ユーザーは、ウイルス、マルウェア、不正侵入を過度に恐れることなく、Appleデバイス上のアプリケーションにアクセスできます。

最も厳重な制御を行うため、iPhone、iPad、iPod touchのアプリケーションは、すべてApp Storeから入手するようになっています。また、すべてのアプリケーションはサンドボックス化されます。

MacでもアプリケーションをApp Storeから入手できますが、インターネットからアプリケーションをダウンロードすることもできます。インターネットからダウンロードする際の安全性を確保するため、macOSには追加の制御レイヤーがあります。まず、macOS 10.15以降では、デフォルトで、Appleの認証を受けていないMacアプリケーションは起動できないようになっています。これにより、App Store以外でアプリケーションを入手する場合でも、それ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。また、macOSにはマルウェアをブロックし、必要に応じて削除する最先端のウイルス対策が施されています。

複数のプラットフォームに設けられた制御機能であるサンドボックス化は、アプリケーションによる不正なアクセスからユーザーのデータを保護するために役立ちます。またmacOSでは、重要な場所にあるデータ自体が保護されています。そのためユーザーは、対象のアプリケーションがサンドボックス化されているかどうかにかかわらず、デスクトップ、書類、ダウンロードなどの場所にあるファイルへのアクセスを確実に制御することができます。

サービスのセキュリティ

Appleは、ユーザーがデバイスでもっと役立つことをしたり、生産性を上げることができるように、多数の堅牢なサービスを構築してきました。こうしたサービスでは、クラウドストレージ、同期、パスワードストレージ、認証、決済、メッセージ、コミュニケーションのためのパワフルな機能を提供する一方で、ユーザープライバシーとデータセキュリティも保護しています。

このようなサービスとして、iCloud、Appleでサインイン、Apple Pay、iMessage、Business Chat、FaceTime、「探す」、連係といったものがあります。これらのサービスを利用するには、Apple ID

または管理対象Apple IDが必要な場合があります。Apple Payなど特定のサービスは、管理対象Apple IDでは利用できません。

注：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。

ネットワークのセキュリティの概要

Appleのデバイスには、保存されたデータを保護するためのセキュリティ機能が搭載されていますが、組織ではそれらに加えて、デバイス間で送受信される情報の安全性を保つために様々な手段を取ることができます。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。

ユーザーにとって、世界中のどこからでも企業の情報ネットワークにアクセスできることは不可欠です。その際には、ユーザーの承認とデータ転送時の保護を確実に行う必要があります。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。

パートナーのエコシステム

Appleのデバイスは、企業が使用する一般的なセキュリティツールやサービスと連係して動作するので、デバイスおよびデバイス上のデータの適合性を保つことができます。ネットワークトラフィックを保護し、一般的なエンタープライズインフラにセキュアに接続するため、各プラットフォームはVPNの標準プロトコル（iOSおよびiPadOS 14のPer Account VPN接続を含む）およびセキュリティ保護されたWi-Fiをサポートしています。

また、AppleはCiscoとの提携によって、両社の製品を組み合わせることでセキュリティと生産性をさらに向上させる機能を提供しています。Cisco Security ConnectorによってCiscoのネットワークのセキュリティが強化され、Ciscoネットワーク上の業務アプリケーションが優先されるようになっています。

Appleのデバイスのセキュリティについて、詳しくは以下を参照してください。

apple.com/jp/business/it

apple.com/jp/macos/security

apple.com/jp/privacy/features

support.apple.com/ja-jp/guide/security