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確保するには、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のデバイスには、セキュリティ機能を備えたチップ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チップなどがありますが、この中で最も重要なコンポーネントがSecure Enclaveコプロセッサで、最新のiOS、iPadOS、watchOS、tvOSデバイスと、Apple T2 Securityチップを搭載したすべてのMacコンピュータに採用されています。Secure Enclaveは、保存されたデータの暗号化、macOSのセキュアブート、生体認証のための基盤を提供します。

最新のiPhone、iPad、およびT2チップを搭載したMacには、ファイルの読み書きと同じ速さで暗号化が可能な専用のAESハードウェアエンジンが内蔵されています。これにより、存続期間の長い暗号鍵をCPUやオペレーティングシステムにさらすことなく、データ保護とFileVaultによってユーザーのファイルを保護することができます。

Appleのデバイスのセキュアブートは、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が提供す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。iOSおよびiPadOSデバイスのセキュリティ確保の基盤となるのは、Boot ROMと呼ばれる変更不可能なコードです。このコードは、チップの製造工程で組み込まれるもので、ハードウェアの信頼性の根幹として知られています。T2チップを搭載したMacコンピュータでは、Secure Enclaveによってセキュアブートを実行する際の信頼性が確認されます。

Secure Enclaveは、AppleのデバイスのTouch IDおよびFace IDを有効にし、ユーザーの生体認証データのプライバシーとセキュリティを保護しながら、セキュア認証を可能にします。これにより、文字数の多い複雑なパスコードとパスワードと同様の安全性を、簡単で迅速な認証方法で確保できるようになります。

Appleのデバイスのセキュリティ機能は、Apple独自のチップ設計、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

Appleのハードウェアの独自機能上に構築されたシステムセキュリティは、使いやすさを損なうことなく、Appleのデバイス上で実行されるオペレーティングシステムのセキュリティを最大化するよう設計されています。システムセキュリティは、起動プロセス、ソフトウェアアップデート、および実行中のオペレーティングシステムを対象にしています。

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コントロールが引き渡されます。このセキュリティモデルでは、Appleのデバイスのデフォルトの起動方法だけでなく、iOS、iPadOS、macOSデバイスの復元やアップデートを行う様々なモードもサポートされています。

最もセキュリティが高いのは、最新バージョンのiOS、iPadOS、macOSです。ソフトウェアアップデートは、Appleのデバイスのアップデートをタイムリーに提供するだけでなく、信頼性の高いソフトウェアだけを提供するための仕組みでもあります。この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。

さらに、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完全性が保たれます。この保護機能は、iOS、iPadOS、macOSデバイスで大きく異なります。サポートする機能に大きな違いがあり、この違いに応じて回避すべき攻撃の種類も異なるためです。

このようなレベルでの保護を実現するために、iOSとiPadOSは、Kernel Integrity Protection、System Coprocessor Integrity、Pointer Authentication Codes、Page Protection Layerを使用しています。macOSでは、Unified Extensible Firmware Interfaceセキュリティ、システム管理モード、Direct Memory Access保護、周辺機器のファームウェアセキュリティを使用しています。

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常時保護されるほか、デバイスの盗難または紛失時にも迅速かつ完全にリモートワイプを実行できる手段が提供されるため、ユーザーと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によって、またMacではFileVaultと呼ばれるボリューム暗号化テクノロジーによってデータを保護しています。どちらのモデルも、キーを管理する階層がデバイス上のSecure Enclaveの専用チップにあり、このチップ上にSEP（Secure Enclave Processor）が搭載されています。両モデルとも専用のAESエンジンによって高速な暗号化に対応しているため、存続期間の長い暗号鍵を、マルウェアに感染する可能性のあるカーネルOSやCPUに提供する必要はありません。

アプリケーションのセキュリティ

アプリケーションは、現代の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は複数の保護レイヤーを構築し、既知のマルウェアへの感染と改ざんからアプリケーションを保護しています。アプリケーションがユーザーデータにアクセスする場合は、このプロセスをOSが注意深く仲介し、別の保護を実行します。

デバイスに内蔵されたセキュリティ管理機能によって、安定したセキュアなアプリケーションの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が数十万ものアプリケーションを、システムの完全性を損なうことなくiOS、iPadOS、macOSに配信することが可能になっています。また、Appleのデバイスにはウイルス、マルウェア、不正な攻撃に対する保護機能があるため、ユーザーはアプリケーションに安心してアクセスすることができます。

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。また厳格に管理するために、すべてのアプリケーションはサンドボックス化されています。Macでも、多くの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には追加のコントロール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、既知のマルウェアに感染することはありません。さらに、macOSには業界標準のウイルス対策が施されているので、マルウェアをブロックし、必要な場合は削除することもできます。

複数のプラットフォームに設けられた管理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サンドボックス化されています。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コントロール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。そのようなサービスには、Apple ID、iCloud、Appleでサインイン、Apple Pay、iMessage、FaceTime、Siri、「探す」アプリケーションなどがあります。こうしたサービスでは、クラウドのストレージおよび同期、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。

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。各プラットフォームはVPNおよびセキュアWi-Fiの標準的なプロトコルに対応しているので、ネットワークトラフィックを保護し、一般的な企業インフラにセキュアに接続することができます。

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/welcome/web（英語）