セキュリティ認証とコンプライアンスセンター

2021年12月

目次

Appleのセキュリティ保証の概要 **4**

ハードウェアの認証 4

ソフトウェアとアプリケーションの認証 5

サービスの認証 5

ハードウェアのセキュリティ認証 **6**

Apple製ハードウェアのセキュリティ認証の概要 6

Secure Enclave Processorのセキュリティ認証 9

Apple T2セキュリティチップのセキュリティ認証 13

オペレーティングシステムのセキュリティ認証 **17**

Appleのオペレーティングシステムのセキュリティ認証の概要 17

iOSのセキュリティ認証 20

iPadOSのセキュリティ認証 27

macOSのセキュリティ認証 33

tvOSのセキュリティ認証 40

watchOSのセキュリティ認証 44

ソフトウェアのセキュリティ認証 **48**

Appleのソフトウェアのセキュリティ認証の概要 48

Apple製アプリケーションのセキュリティ認証 50

Appleのインターネットサービスのセキュリティ認証 **53**

ISO/IEC 27001 53

ISO/IEC 27018 54

ISO/IEC 27001およびISO/IEC 27018が適用されるAppleのサービス 54

認証取得 55

macOSセキュリティ・コンプライアンス・プロジェクト 56

ドキュメントの改訂履歴 57

用語集 58

Appleのセキュリティ保証の概要

Appleは、セキュリティへの取り組みの一環として、定期的に第三者組織と連携して、Appleのハードウェア、ソフトウェア、およびサービスのセキュリティの認証および実証を行っています。Appleは、オペレーティングシステムのメジャーリリースに合わせて、国際的に認められている組織から認証を取得しています。これにより、システムのセキュリティニーズが満たされているという信頼（つまり、セキュリティ保証）が与えられます。相互承認協定（MRA）の対象外、またはまだセキュリティ認証規格が十分に確立されていない技術領域については、Appleは適切なセキュリティ規格の開発に取り組んでいます。Appleのミッションは、Appleのすべてのハードウェア、オペレーティングシステム、アプリケーション、およびサービスについて、グローバルに認められた包括的なセキュリティ認証を取得できるようにすることです。

多くの場合、認証を取得するには、法律、規制、業界基準の要件を満たす必要があります。Apple School ManagerやApple Business Managerなどのサービスは、Appleが取得したISO/IEC 27001およびISO/IEC 27018の認証に準拠しています。ハードウェア、オペレーティングシステム、ソフトウェア、およびサービスの認証により、Appleデバイスを導入している政府機関、企業、教育機関を含むすべてのお客様のコンプライアンス準拠が証明されます。

ハードウェアの認証

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内蔵されたセキュリティ基盤が必要なため、すべてのAppleデバイスは（iOS、iPadOS、macOS、tvOS、watchOSのいずれが動作しているかに関係なく）、シリコンにセキュリティ機能が組み込まれるように設計されています。これには、システムのセキュリティ機能を強化するカスタムCPU機能や、セキュリティ機能専用のシリコンが含まれます。最も重要なコンポーネントは、Secure Enclaveコプロセッサで、これは最新のすべてのiOS、iPadOS、watchOS、tvOSデバイス、Appleシリコンを搭載したすべてのMacコンピュータ、およびApple T2セキュリティチップを搭載したIntelベースのすべてのMacコンピュータに存在します。Secure Enclaveにより、保存されたデータの暗号化、macOSのセキュアブート、および生体認証が提供されます。

Appleのセキュリティ保証への取り組みは、ハードウェアの信頼の起点からセキュアブートの適用、Secure Key Storeを提供するSecure Enclave、Touch IDやFace IDによる安全な認証にいたるまで、シリコン内の基礎的なセキュリティコンポーネントの認証を取得することから始まります。Appleデバイスのセキュリティ機能は、シリコンの設計、ハードウェア、ソフトウェア、およびAppleからのみ利用可能なサービスを組み合わせることによって実現されています。これらのコンポーネントの認証は、Appleが提供する保証を実証する上で重要な要素です。

ハードウェアおよび関連するファームウェアコンポーネントに関する公的認証については、以下を参照してください:

- Apple T2セキュリティチップのセキュリティ認証
- Secure Enclave Processorのセキュリティ認証

ソフトウェアとアプリケーションの認証

Appleは、暗号モジュールについては米国連邦情報処理規格（FIPS）140-2/-3、オペレーティングシステム、アプリケーション、デバイスのサービスについてはコモンクライテリアに基づく独立した認証と証明を取得および維持しています。対象となるオペレーティングシステムには、iOS、iPadOS、macOS、sepOS、T2ファームウェア、tvOS、およびwatchOSが含まれます。アプリケーションについては、Safariブラウザと「連絡先」の認証を個別に取得しますが、今後はほかのアプリケーションの認証も取得していきます。

Appleの**オペレーティングシステム**に関する公的認証については、以下を参照してください:

- iOSのセキュリティ認証
- iPadOSのセキュリティ認証
- macOSのセキュリティ認証
- tvOSのセキュリティ認証
- watchOSのセキュリティ認証

Apple製**アプリケーション**に関する公的認証については、以下を参照してください:

- Apple製アプリケーションのセキュリティ認証

サービスの認証

Appleは、企業から教育機関にいたるまでのお客様をサポートするためにセキュリティ認証を維持しています。このような認証により、Appleをご利用のお客様はAppleのハードウェアおよびソフトウェアでAppleのサービスを使用するときに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、Appleのシステムに対するAppleの情報セキュリティの確保、環境保全、およびプライバシー保護の実践が自ずと証明されることになります。

Appleの**インターネットサービス**に関する公的認証については、以下を参照してください:

- Appleのインターネットサービスのセキュリティ認証

Appleのセキュリティとプライバシーの認証についての質問は、security-certifications@apple.comにお問い合わせください。

ハードウェアのセキュリティ認証

Apple製ハードウェアのセキュリティ認証の概要

Appleは、sepOSおよびT2ファームウェアについて、米国連邦情報処理規格（FIPS）140-2/-3認証証明書およびその他の証明書を取得し、維持しています。Appleでは、該当する複数のプラットフォームに広く適用される**認証構成要素**から取り組みを始めています。構成要素の1つ目は、ソフトウェアおよびハードウェアの暗号モジュールをAppleが開発するオペレーティングシステム内に展開するために使用されるcorecryptoライブラリの認証です。構成要素の2つ目は、多くのAppleデバイスに内蔵されているSecure Enclaveの認証です。3つ目は、Touch IDを搭載したAppleデバイスとFace IDを搭載したデバイスに採用されているSecure Element（SE）の認証です。これらのハードウェア認証構成要素が、より広範なプラットフォームセキュリティ認証の基礎となります。

暗号アルゴリズムの認証

多くの暗号アルゴリズムおよび関連セキュリティ機能の実装の正確性に関する認証は、FIPS 140-3認証の前提条件であり、ほかの認証の裏付けとなります。認証は、アメリカ国立標準技術研究所（NIST）の暗号アルゴリズム認証制度（CAVP）によって管理されています。Appleの実装に関する認証証明書は、CAVPの検索サイトで確認できます。詳しくは、暗号アルゴリズム認証制度（CAVP）のWebサイトを参照してください。

暗号モジュールの認証: FIPS 140-2/3(ISO/IEC 19790)

Appleの暗号モジュールは、2012年以降、オペレーティングシステムのメジャーリリースのたびに暗号モジュール用の米国連邦情報処理規格(FIPS140-2)に準拠していることが暗号モジュール認証制度(CMVP)によって認証されています。毎回のメジャーリリース後に、Appleは規格適合の認証を受けるためにCMVPにモジュールを提出しています。これらのモジュールは、Appleのオペレーティングシステムやアプリケーションで使用されるだけでなく、Appleが提供するサービスに暗号機能を提供しており、他社製のアプリケーションでも使用できます。

Appleは、毎年、macOS用のソフトウェアベースのモジュールである「Intel用Corecryptoモジュール」と「Intel用Corecryptoカーネルモジュール」について**セキュリティレベル1**を満たしています。Appleシリコンについては、「ARM用Corecryptoモジュール」と「ARM用Corecryptoカーネルモジュール」のモジュールが、iOS、iPadOS、tvOS、watchOS、およびMacコンピュータに内蔵されているApple T2セキュリティチップのファームウェアに適用されます。

2019年、Appleは「Apple CoreCryptoモジュール: Secure Key Store」と呼ばれる組み込みハードウェア暗号モジュールについて、初のFIPS 140-2**セキュリティレベル2**を達成しました。これによって、Secure Enclaveで生成および管理される鍵の使用が米国政府に承認されました。Appleは、今後のオペレーティングシステムのメジャーリリースでも、ハードウェア暗号モジュールに関する認証の取得を目指します。

2019年にアメリカ合衆国商務省によって**FIPS 140-3**が承認されました。今回の改訂で最も大きく変わった点は、ISO/IEC規格(特にISO/IEC 19790:2015)と、これに関連する試験要件を定めたISO/IEC 24759:2017の仕様です。CMVPでは移行プログラムが開始されていて、2020年にはFIPS 140-3に基づく暗号モジュールの検証が始まることが表明されています。Appleは、暗号モジュールができる限り速やかにFIPS 140-3標準を満たすこと、およびFIPS 140-3標準に移行することを目指しています。

現在テストおよび認定プロセス中の暗号モジュールについては、CMVPによって申請中の認定に関する情報が含まれた2つのリストを公開しています。公認試験機関でテスト中の暗号モジュールは、「Implementation Under Test List」に記載されています。試験機関でテストが実施され、CMVPによる認定が勧告されると、Appleの暗号モジュールが「Modules in Process List」に掲載されます。現在、試験機関でのテストが完了し、CMVPによるテストの認定を待機中です。評価プロセスの長さは変わる可能性があるため、オペレーティングシステムのメジャーリリース日からCMVPによる認証証明書の発行日までの間にAppleの暗号モジュールの現在の状況を確認する場合は、上記の2つのリストを参照してください。

製品の認証:(コモンクライテリアISO/IEC 15408)

コモンクライテリア(ISO/IEC 15408)は、多くの組織でIT製品のセキュリティ評価を実施するための基礎として使用されている標準規格です。

国際的なコモンクライテリア承認協定(CCRA)のもとで相互承認されている認証については、コモンクライテリアのポータルサイトを参照してください。コモンクライテリアの規格は、CCRA外でも国や私的機関の認定スキームに使用されることがあります。欧州では、SOG-IS協定およびCCRAのもとで相互承認が管理されています。

コモンクライテリア・コミュニティが示している通り、目標は、国際的に承認されている一連のセキュリティ規格によって、明確で信頼できるIT製品のセキュリティ機能の評価を行うことです。コモンクライテリア認証により、製品の機能がセキュリティ規格を満たしているかどうかの独立した評価が与えられるため、IT製品のセキュリティに対する信頼性が向上し、ユーザはより確かな情報に基づいた意思決定を行うことができます。

CCRAを通じて、加盟国は、一貫した信頼レベルにてIT製品の認証を承認することに同意しています。認証前に必要な評価は多岐にわたり、以下のようなものがあります:

- プロテクションプロファイル(PP)
- セキュリティターゲット(ST)
- セキュリティ機能要件(SFR)
- セキュリティ保証要件(SAR)
- 評価保証レベル(EAL)

プロテクションプロファイル（PP）とはデバイスタイプ（モバイルなど）のクラスのセキュリティ要件を指定する書類のことであり、同じクラスに属する異なるIT製品の評価を比較可能にするために使用されます。CCRAの加盟国や加盟地域は、承認されたPPのリストの増大に伴い毎年増え続けています。この協定により、製品のデベロッパは、いずれか1つの認証承認スキーム下で1つの認証を取得すれば、その認証を受け入れるすべての署名国や署名地域で承認されることになります。

セキュリティターゲット（ST）では、IT製品の認証時に評価される**項目**を定義します。STは、STを詳細に評価するために使用される、より具体的な**セキュリティ機能要件（SFR）**に変換されます。

コモンクライテリア（CC）でも**セキュリティ保証要件**を定めています。一般的に認定されている指標の1つが**評価保証レベル（EAL）**です。EALは、よく使われる一連のSARをまとめたもので、比較検証に対応するためにPPおよびSTで指定されることがあります。

過去のPPの多くはアーカイブされており、特定の解決策や環境に焦点を当てて作成された、対象となるPPに置き換えられています。すべてのCCRA加盟国や加盟地域が継続的に相互承認を行えるように協力する中、collaborative Protection Profiles（cPP）の開発と保守のためにinternational Technical Community（iTC）が設立されました。cPPは、はじめからCCRAの署名スキームに対応するように開発されます。CCRA以外のユーザグループや相互承認協定を対象としたPPは、引き続き該当するステークホルダによって開発されます。

Appleは、2015年初旬より、特定のcPPについて、アップデートされたCCRAに基づく認証の取得を目指し始めました。それ以来、AppleはiOSのメジャーリリースごとにコモンクライテリア認証を取得し、新しいPPによって定義されるセキュリティ保証の実現にまで対応範囲を広げてきました。

Appleは、モバイルセキュリティテクノロジーを評価する技術コミュニティで積極的な役割を果たしています。このようなコミュニティには、cPPの開発とアップデートを行うiTCが含まれます。Appleは今後も、現在のPPおよびcPPの評価と、それに基づいた認証を目指していきます。

北米市場のAppleプラットフォームの認証は、通常、国家情報保証パートナーシップ（NIAP）が行います。NIAPは、まだ認証されていない現在評価中のプロジェクトのリストを管理しています。

リストに掲載されている一般的なプラットフォームの認証に加え、一部の市場向けの特定のセキュリティ要件を示すために、その他の認証も発行されています。

Secure Enclave Processorのセキュリティ認証

Secure Enclave認証取得の背景

ハードウェア暗号モジュール(**Apple SEP Secure Key Store Cryptographic Module**)は、AppleのAシリーズ(iPhoneおよびiPad用)、Mシリーズ(Appleシリコン搭載Macコンピュータ用)、Sシリーズ(Apple Watch用)、およびTシリーズのセキュリティチップ(2017年に発売されたiMac Pro以降のIntelベースのMacコンピュータに搭載)といった製品のApple SOCに内蔵されています。

2018年には、2017年にリリースされたオペレーティングシステム(iOS 11、macOS 10.13、tvOS 11、watchOS 4)のソフトウェア暗号モジュールの認証との整合性を図りました。Apple SEP Secure Key Store Cryptographic Module v1.0として識別されたSEPハードウェア暗号モジュールは当初、FIPS 140-2セキュリティレベル1の要件を満たし、認証されました。

2019年、Appleは、ハードウェアモジュールがFIPS 140-2セキュリティレベル2の要件を満たしたとして認証を取得し、対応するcorecryptoユーザモジュールとcorecryptoカーネルモジュールの認証済みバージョンとの整合性を図るため、モジュールのバージョン識別子をv9.0にアップデートしました。2019年には、iOS 12、macOS 10.14、tvOS 12、およびwatchOS 5が対象となっています。

2020年と2021年には、AppleはFIPS 140-3への準拠、およびAppleシリコン(A13、A14、S6、M1チップ)の物理的セキュリティ要件であるセキュリティレベル3の追加保証のための認証取得に取り組んでいます。

またAppleは、オペレーティングシステムのメジャーリリースのたびに、corecryptoユーザモジュールとcorecryptoカーネルモジュールの認証取得に積極的に取り組んでいます。適合の認証は、最終公開バージョンに対してのみ実施可能です。

暗号モジュールの認証状況

暗号モジュール認証制度(CMVP)では、暗号モジュールの認証状況を、現在の状況に応じて3つの個別のリストで管理しています:

- CMVPの「Implementation Under Test List」に掲載されるには、試験機関がAppleからテストの実施を請け負う必要があります。
- 試験機関でのテストが完了すると、試験機関からCMVPによる認証が勧告されます。CMVPの手数料が支払われると、モジュールが「Modules in Process List」に追加されます。「MIP List」では、CMVPによる認証対応の進捗状況を以下の4段階で示しています:
    - **Review Pending:** CMVPのリソース割り当てを待機中です。
    - **In Review:** CMVPのリソースが認証活動を実施中です。
    - **Coordination:** 見つかった問題を試験機関とCMVPで解決中です。
    - **Finalization:** 認証書の発行に関連する活動と手続き。
- CMVPによる認証後、モジュールは適合証明書を受け、認証済みの暗号モジュールリストに追加されます。これには次のものが含まれます:
    - 認証済みのモジュールはactiveとしてマークされます。
    - 5年が経過すると、モジュールはhistoricalとしてマークされます。
    - 何らかの理由でモジュールの認証書が取り消された場合、モジュールはrevokedとしてマークされます。

2020年、CMVPはFIPS 140-3のベースとして国際規格のISO/IEC 19790を採用しました。

FIPS 140-3の認証

現在の状況

次の表に、現在試験機関でFIPS 140-3への適合を審査中の2020年および2021年の暗号モジュールを示します。

2020年および2021年のオペレーティングシステムのリリースに関するSecure Key Store（SKS）は、試験機関でのテストが完了し、試験機関からCMVPへ認証が勧告されています。これらは、「Modules in Process List」に掲載されており、認証されると認証済みの暗号モジュールリストに移されます。

iOS 15（2021年）のユーザ空間、カーネル空間、Secure Key Storeは、試験機関でのテストが進行中です。これらは、「Implementation Under Test List」に掲載されています。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple corecrypto Module v12 **オペレーティングシステム:** 2021年にリリースされるiOS、iPadOS、macOS、tvOS、およびwatchOSと共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（A9-A14、T2、M1、S3-S6） **全体的なセキュリティレベル:** 2
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** 2021年にリリースされるiOS、iPadOS、macOS、tvOS、およびwatchOSと共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（A13、A14、S6、M1） **全体的なセキュリティレベル:** 2 **物理的セキュリティレベル:** 3
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** 2020年にリリースされるiOS、iPadOS、macOS、tvOS、およびwatchOSと共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（A9-A14、T2、M1、S3-S6） **全体的なセキュリティレベル:** 2
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** 2020年にリリースされるiOS、iPadOS、macOS、tvOS、およびwatchOSと共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（A13、A14、S6、M1） **全体的なセキュリティレベル:** 2 **物理的セキュリティレベル:** 3

FIPS 140-2の認証

次の表に、試験機関でFIPS 140-2への適合を審査された暗号モジュールを示します。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2019 **認証日:** 2021/02/05	**認証書:** 3811 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v10.0 **オペレーティングシステム:** macOS 10.15 CatalinaのsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/09/10	**認証書:** 3523 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v9.0 **オペレーティングシステム:** macOS 10.14 MojaveのsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2017 **認証日:** 2019/09/10	**認証書:** 3223 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v1.0 **オペレーティングシステム:** macOS 10.13 High SierraのsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2

コモンクライテリア(CC)認証

Appleは、適切なプロテクションプロファイルがAppleテクノロジーのセキュリティ機能をカバーする、コモンクライテリア認証の取得に積極的に取り組んでいます。

コモンクライテリア(CC)認証の取得状況

NIAPが運営している米国スキームでは、「Products in Evaluation」というリストが管理されており、現在米国でNIAPの認定を受けたCommon Criteria Testing Laboratory(CCTL)による評価が進行中の製品、およびCCEVSの責任者により製品が正式に受理されて評価が開始されるEvaluation Kickoff Meeting(またはこれに相当するもの)が完了した製品が記載されています。

製品が認証されると、NIAPにより、現在有効な認証を持つ製品がNIAPの「Product Compliant List」に掲載されます。2年が経過した認証製品は、現在の保証維持ポリシーに従って再審査されます。保証維持期限が切れた認証は、NIAPの「Archived Products」リストに移ります。

コモンクライテリアのポータルには、コモンクライテリア承認協定(CCRA)のもとで相互承認可能な認証製品が掲載されています。コモンクライテリアのポータルの認証済み製品のリストには製品が5年間掲載されます。アーカイブ済みの認証製品については、コモンクライテリアのポータルに記録が残ります。

次の表に、現在試験機関で評価中の製品、またはコモンクライテリアに適合しているとして認証された製品を示します。

オペレーティングシステム/認証日	スキームID/書類	タイトル/プロテクションプロファイル
オペレーティングシステム: sepOS **認証日:** —	**スキームID:** まだ認証されていません **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** Apple Secure Enclave [2020] **プロテクションプロファイル:** CPP_DSC_V1.0 **ハードウェア:** Secure Enclave（A9-A14、M1、T2、S3-S6） **ソフトウェア:** iOS 14、iPadOS 14、macOS 11 Big Sur、tvOS 14、watchOS 7と共に配布されるsepOS

その他の認証

次の表に、コモンクライテリアもFIPS140-3も使用しないSecure Enclaveの認証を示します。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2020 **認証日:** 2019/12/07〜2022/12/26	**認証書:** CFNR201902910002（中華人民共和国：モバイル金融サービスの技術認証） 中国語版 英語版	**タイトル:** モバイル端末の信頼できる実行環境 **オペレーティングシステム:** iOS 13.5.1 **仕様:** JR/T 0156-2017

Apple T2セキュリティチップのセキュリティ認証

暗号モジュールの認証取得の背景

Appleは、オペレーティングシステムのメジャーリリースのたびに、Appleの内蔵ソフトウェアおよびハードウェアモジュールの認証取得に積極的に取り組んでいます。適合の認証は、最終モジュールの公開バージョンに対してのみ実施可能です。

2020年、CMVPは米国連邦情報処理規格(FIPS)140-3のベースとして国際規格のISO/IEC 19790を採用しました。

Intel CPUに加えて、2017年以降のほとんどのMacコンピュータもAppleシリコンベースのSystem on Chip(SoC)であるApple T2セキュリティチップを搭載しています。これらのT2チップを搭載しているMacコンピュータでは、デバイス上のさまざまなサービスに5つの暗号モジュールをすべて使用しています。

- Intel用Corecryptoユーザモジュール(IntelベースのMacコンピュータ上のmacOSで使用)
- Intel用Corecryptoカーネルモジュール(IntelベースのMacコンピュータ上のmacOSで使用)
- ARM用Corecryptoユーザモジュール(T2チップで使用)
- ARM用Corecryptoカーネルモジュール(T2チップで使用)
- Secure Key Store Cryptographic Module(T2チップの組み込みSecure Enclaveコプロセッサで使用)

注記: T2チップ上で動作するAppleシリコンベースのモジュールは、AppleのAシリーズ、Sシリーズ、Mシリーズなど、ほかのAppleシリコンで動作するものと同じです。

暗号モジュールの認証状況

暗号モジュール認証制度(CMVP)では、暗号モジュールの認証状況を、現在の状況に応じて3つの個別のリストで管理しています:

- CMVPの「Implementation Under Test List」に掲載されるには、試験機関がAppleからテストの実施を請け負う必要があります。
- 試験機関でのテストが完了すると、試験機関からCMVPによる認証が勧告されます。CMVPの手数料が支払われると、モジュールが「Modules in Process(MIP)List」に追加されます。「MIP List」では、CMVPによる認証対応の進捗状況を以下の4段階で示しています:
  - **Review Pending:** CMVPのリソース割り当てを待機中です。
  - **In Review:** CMVPのリソースが認証活動を実施中です。
  - **Coordination:** 見つかった問題を試験機関とCMVPで解決中です。
  - **Finalization:** 認証書の発行に関連する活動と手続き。
- CMVPによる認証後、モジュールは適合証明書を受け、認証済みの暗号モジュールリストに追加されます。これには次のものが含まれます:
  - 認証済みのモジュールはactiveとしてマークされます。
  - 5年が経過すると、モジュールはhistoricalとしてマークされます。
  - 何らかの理由でモジュールの認証書が取り消された場合、モジュールはrevokedとしてマークされます。

FIPS 140-3の認証

現在の状況

2020年のモジュールのユーザ空間、カーネル空間、Secure Key Storeは、試験機関でのテストが完了し、試験機関からCMVPへ認証が勧告されています。これらは、「Modules in Process List」に掲載されています。

2021年のモジュールのユーザ空間、カーネル空間、Secure Key Storeは、試験機関で試験が進行中です。これらは、「Implementation Under Test List」に掲載されています。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12.0 **オペレーティングシステム:** macOS 12 MontereyのsepOS **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12.0 **オペレーティングシステム:** macOS 12 MontereyのsepOS **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12.0 **オペレーティングシステム:** macOS 12 MontereyのsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(T2) **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** macOS 11 Big SurのsepOS **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** macOS 11 Big SurのsepOS **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** Intel上のmacOS 11 Big SurのsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア **セキュリティレベル:** 2

FIPS 140-2の認証

次の表に、試験機関でFIPS 140-2への適合を審査された暗号モジュールを示します。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2019 **認証日:** 2021年3月23日	**認証書:** 3856 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v10.0 for ARM **オペレーティングシステム:** macOS 10.15 CatalinaのsepOS **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** 2021年3月23日	**認証書:** 3855 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v10.0 for ARM **オペレーティングシステム:** macOS 10.15 CatalinaのsepOS **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** 2021/02/05	**認証書:** 3811 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Secure Key Store Cryptographic Module v10.0 **オペレーティングシステム:** macOS 10.15 CatalinaのsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/23	**認証書:** 3438 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v9.0 for ARM **オペレーティングシステム:** macOS 10.14 MojaveのsepOS **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/11	**認証書:** 3433 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v9.0 for ARM **オペレーティングシステム:** macOS 10.14 MojaveのsepOS **タイプ:** ソフトウェア **セキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/09/10	**認証書:** 3523 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v9.0 **オペレーティングシステム:** macOS 10.14 MojaveのsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/09、2018/05/22、2018/07/06	**認証書:** 3148 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v8.0 for ARM **オペレーティングシステム:** macOS 10.13 High SierraのsepOS **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/09、2018/05/17、2018/07/03	**認証書:** 3147 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v8.0 for ARM **オペレーティングシステム:** macOS 10.13 High SierraのsepOS **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/07/10	**認証書:** 3223 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v1.0 **オペレーティングシステム:** macOS 10.13 High SierraのsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2016 **認証日:** 2017/02/01	**認証書:** 2828 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple iOS Corecrypto Kernel Module v7.0 **オペレーティングシステム:** macOS 10.12 SierraのsepOS **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2016 **認証日:** 2017/02/01	**認証書:** 2827 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple iOS Corecrypto Kernel Module v7.0 **オペレーティングシステム:** macOS 10.12 SierraのsepOS **タイプ:** ソフトウェア **セキュリティレベル:** 1

オペレーティングシステムのセキュリティ認証

Appleのオペレーティングシステムのセキュリティ認証の概要

Appleは、sepOSおよびT2ファームウェアについて、米国連邦情報処理規格（FIPS）140-2/-3認証証明書およびその他の証明書を取得し、維持しています。Appleでは、該当する複数のプラットフォームに広く適用される**認証構成要素**から取り組みを始めています。構成要素の1つ目は、ソフトウェアおよびハードウェアの暗号モジュールをAppleが開発するオペレーティングシステム内に展開するために使用されるcorecryptoの認証です。構成要素の2つ目は、多くのAppleデバイスに内蔵されているSecure Enclaveの認証です。3つ目は、Touch IDを搭載したAppleデバイスとFace IDを搭載したデバイスに採用されているSecure Element（SE）の認証です。これらのハードウェア認証構成要素が、より広範なプラットフォームセキュリティ認証の基礎となります。

暗号アルゴリズムの認証

多くの暗号アルゴリズムおよび関連セキュリティ機能の実装の正確性に関する認証は、FIPS 140-3認証の前提条件であり、ほかの認証の裏付けとなります。認証は、NISTの暗号アルゴリズム認証制度（CAVP）によって管理されています。Appleの実装に関する認証証明書は、CAVPの検索サイトで確認できます。

暗号モジュールの認証: FIPS 140-2/3（ISO/IEC 19790）

Appleのオペレーティングシステムの暗号モジュールは、2012年以降、オペレーティングシステムのメジャーリリースのたびに米国連邦情報処理規格（FIPS）140-2に準拠していることが暗号モジュール認証制度（CMVP）によって認定されています。毎回メジャーリリース後に、Appleは完全な暗号モジュールの認定のためにCMVPにすべてのモジュールを提出しています。これらの認定されたモジュールによってAppleが提供するサービスでの暗号演算が実現します。他社製Appでもこれらのモジュールを使用できます。

Appleは、毎年、macOS用のソフトウェアベースのモジュールである「Intel用Corecryptoモジュール」と「Intel用Corecryptoカーネルモジュール」について**セキュリティレベル1**を満たしています。Appleシリコンについては、「ARM用Corecryptoモジュール」と「ARM用Corecryptoカーネルモジュール」のモジュールが、iOS、iPadOS、tvOS、watchOS、およびMacコンピュータに内蔵されているApple T2セキュリティチップのファームウェアに適用されます。

2019年、Appleは「Apple CoreCryptoモジュール: Secure Key Store」と呼ばれる組み込みハードウェア暗号モジュールについて、初のFIPS 140-2**セキュリティレベル2**を達成しました。これによって、Secure Enclaveで生成および管理される鍵の使用が米国政府に承認されました。Appleは、今後のオペレーティングシステムのメジャーリリースでも、ハードウェア暗号モジュールに関する認証の取得を目指します。

2019年にアメリカ合衆国商務省によって**FIPS 140-3**が承認されました。今回の改訂で最も大きく変わった点は、ISO/IEC規格（特にISO/IEC 19790:2015）と、これに関連する試験要件を定めたISO/IEC 24759:2017の仕様です。CMVPでは移行プログラムが開始されていて、2020年にはFIPS 140-3に基づく暗号モジュールの検証が始まることが表明されています。Appleは、暗号モジュールができる限り速やかにFIPS 140-3標準を満たすこと、およびFIPS 140-3標準に移行することを目指しています。

現在テストおよび認定プロセス中の暗号モジュールについては、CMVPによって申請中の認定に関する情報が含まれた2つのリストを公開しています。公認試験機関でテスト中の暗号モジュールは、「Implementation Under Test List」に記載されています。試験機関でテストが実施され、CMVPによる認定が勧告されると、Appleの暗号モジュールが「Modules in Process List」に掲載されます。現在、試験機関でのテストが完了し、CMVPによるテストの認定を待機中です。評価プロセスの長さは変わる可能性があるため、オペレーティングシステムのメジャーリリース日からCMVPによる認証証明書の発行日までの間にAppleの暗号モジュールの現在の状況を確認する場合は、上記の2つのリストを参照してください。

製品の認証:(コモンクライテリアISO/IEC 15408)

コモンクライテリア(ISO/IEC 15408)は、多くの組織でIT製品のセキュリティ評価を実施するための基礎として使用されている標準規格です。

国際的なコモンクライテリア承認協定(CCRA)のもとで相互承認されている認証については、コモンクライテリアのポータルサイトを参照してください。コモンクライテリアの規格は、CCRA外でも国や私的機関の認定スキームに使用されることがあります。欧州では、SOG-IS協定およびCCRAのもとで相互承認が管理されています。

コモンクライテリア・コミュニティが示している通り、目標は、国際的に承認されている一連のセキュリティ規格によって、明確で信頼できるIT製品のセキュリティ機能の評価を行うことです。コモンクライテリア認証により、製品の機能がセキュリティ規格を満たしているかどうかの独立した評価が与えられるため、IT製品のセキュリティに対する信頼性が向上し、ユーザはより確かな情報に基づいた意思決定を行うことができます。

CCRAを通じて、加盟国は、一貫した信頼レベルにてIT製品の認証を承認することに同意しています。認証前に必要な評価は多岐にわたり、以下のようなものがあります:

- プロテクションプロファイル(PP)
- セキュリティターゲット(ST)
- セキュリティ機能要件(SFR)
- セキュリティ保証要件(SAR)
- 評価保証レベル(EAL)

プロテクションプロファイル(PP)とはデバイスタイプ(モバイルなど)のクラスのセキュリティ要件を指定する書類のことであり、同じクラスに属する異なるIT製品の評価を比較可能にするために使用されます。CCRAの加盟国や加盟地域は、承認されたPPのリストの増大に伴い毎年増え続けています。この協定により、製品のデベロッパは、いずれか1つの認証承認スキーム下で1つの認証を取得すれば、その認証を受け入れるすべての署名国や署名地域で承認されることになります。

セキュリティターゲット(ST)では、IT製品の認証時に評価される**項目**を定義します。STは、STを詳細に評価するために使用される、より具体的な**セキュリティ機能要件(SFR)**に変換されます。

コモンクライテリア(CC)でも**セキュリティ保証要件**を定めています。一般的に認定されている指標の1つが**評価保証レベル(EAL)**です。EALは、よく使われる一連のSARをまとめたもので、比較検証に対応するためにPPおよびSTで指定されることがあります。

過去のPPの多くはアーカイブされており、特定の解決策や環境に焦点を当てて作成された、対象となるPPに置き換えられています。すべてのCCRA加盟国や加盟地域が継続的に相互承認を行えるように協力する中、**collaborative Protection Profiles(cPP)**の開発と保守のためにinternational Technical Community(iTC)が設立されました。cPPは、はじめからCCRAの署名スキームに対応するように開発されます。CCRA以外のユーザグループや相互承認協定を対象としたPPは、引き続き該当するステークホルダによって開発されます。

Appleは、2015年初旬より、特定のcPPについて、アップデートされたCCRAに基づく認証の取得を目指し始めました。それ以来、AppleはiOSのメジャーリリースごとにコモンクライテリア認証を取得し、新しいPPによって定義されるセキュリティ保証の実現にまで対応範囲を広げてきました。

Appleは、モバイルセキュリティテクノロジーを評価する技術コミュニティで積極的な役割を果たしています。このようなコミュニティには、cPPの開発とアップデートを行うiTCが含まれます。Appleは今後も、現在のPPおよびcPPの評価と、それに基づいた認証を目指していきます。

北米市場のAppleプラットフォームの認証は、通常、国家情報保証パートナーシップ（NIAP）が行います。NIAPは、まだ認証されていない現在評価中のプロジェクトのリストを管理しています。

リストに掲載されている一般的なプラットフォームの認証に加え、一部の市場向けの特定のセキュリティ要件を示すために、その他の認証も発行されています。

iOSのセキュリティ認証

iOS認証取得の背景

Appleは、オペレーティングシステムのメジャーリリースのたびに、Appleの内蔵ソフトウェアおよびハードウェアモジュールの認証取得に積極的に取り組んでいます。適合の認証は、最終公開バージョンに対してのみ実施可能です。

iOSの暗号モジュールの認証状況

暗号モジュール認証制度(CMVP)では、暗号モジュールの認証状況を、現在の状況に応じて3つの個別のリストで管理しています:

- CMVPの「Implementation Under Test List」に掲載されるには、試験機関がAppleからテストの実施を請け負う必要があります。
- 試験機関でのテストが完了すると、試験機関からCMVPによる認証が勧告されます。CMVPの手数料が支払われると、モジュールが「Modules in Process(MIP)List」に追加されます。「MIP List」では、CMVPによる認証対応の進捗状況を以下の4段階で示しています:
  - **Review Pending:** CMVPのリソース割り当てを待機中です。
  - **In Review:** CMVPのリソースが認証活動を実施中です。
  - **Coordination:** 見つかった問題を試験機関とCMVPで解決中です。
  - **Finalization:** 認証書の発行に関連する活動と手続き。
- CMVPによる認証後、モジュールは適合証明書を受け、認証済みの暗号モジュールリストに追加されます。これには次のものが含まれます:
  - 認証済みのモジュールはactiveとしてマークされます。
  - 5年が経過すると、モジュールはhistoricalとしてマークされます。
  - 何らかの理由でモジュールの認証書が取り消された場合、モジュールはrevokedとしてマークされます。

2020年、CMVPはFIPS 140-3のベースとして国際規格のISO/IEC 19790を採用しました。

FIPS 140-3の認証

現在の状況

iOS 14（2020年）のユーザ空間、カーネル空間、Secure Key Storeは、試験機関でのテストが完了し、試験機関からCMVPへ認証が勧告されています。これらは、「Modules in Process List」に掲載されています。

iOS 15（2021年）のユーザ空間、カーネル空間、Secure Key Storeは、試験機関での試験が進行中です。これらは、「Implementation Under Test List」に掲載されています。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** iOS 15 **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** iOS 15 **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** iOS 15と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（A9-A14） **全体的なセキュリティレベル:** 2
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** iOS 15と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（A13、A14、A15） **全体的なセキュリティレベル:** 2 **物理的セキュリティレベル:** 3
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** iOS 14 **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** iOS 14 **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** iOS 14と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(A9-A14) **全体的なセキュリティレベル:** 2
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** iOS 14と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(A13-A14) **全体的なセキュリティレベル:** 2 **物理的セキュリティレベル:** 3

FIPS 140-2の認証

次の表に、試験機関でFIPS 140-2への適合を現在審査中および審査済みの暗号モジュールを示します。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2019 **認証日:** 2021年3月23日	**認証書:** 3856 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v10.0 for ARM **オペレーティングシステム:** iOS 13 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** 2021年3月23日	**認証書:** 3855 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v10.0 for ARM **オペレーティングシステム:** iOS 13 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** 2021/02/05	**認証書:** 3811 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v10.0 **オペレーティングシステム:** iOS 13と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/23	**認証書:** 3438 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v9.0 for ARM **オペレーティングシステム:** iOS 12 **タイプ:** ソフトウェア **セキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/11	**認証書:** 3433 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v9.0 for ARM **オペレーティングシステム:** iOS 12 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/09/10	**認証書:** 3523 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v9.0 **オペレーティングシステム:** iOS 12と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/09、2018/05/22、2018/07/06	**認証書:** 3148 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v8.0 for ARM **オペレーティングシステム:** iOS 11 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/09、2018/05/17、2018/07/03	**認証書:** 3147 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v8.0 for ARM **オペレーティングシステム:** iOS 11 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2019/09/10	**認証書:** 3223 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v1.0 **オペレーティングシステム:** iOS 11と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2016 **認証日:** 2017/02/01	**認証書:** 2828 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple iOS Corecrypto Kernel Module v7.0 **オペレーティングシステム:** iOS 10 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2016 **認証日:** 2017/02/01	**認証書:** 2827 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple iOS Corecrypto Kernel Module v7.0 **オペレーティングシステム:** iOS 10 **タイプ:** ソフトウェア **セキュリティレベル:** 1

以前のバージョン

5年以上が経過した認証書は、CMVPの履歴リストに掲載されています。以下に示す以前のバージョンのiOSについては、暗号モジュールの認証を取得済みです:

- iOS 9(corecryptoモジュールv6.0)
- iOS 8(corecryptoモジュールv5.0)
- iOS 7(corecryptoモジュールv4.0)
- iOS 6(corecryptoモジュールv3.0)

コモンクライテリア(CC)認証取得の背景

Appleは、オペレーティングシステムのメジャーリリースのたびに、iOSの認証取得に積極的に取り組んでいます。認証は、最終公開バージョンに対してのみ実施可能です。iPadOS 13.1より前は、iPadOSはiOSという名称でした。

コモンクライテリア(CC)認証の取得状況

NIAPが運営している米国スキームでは、「Products in Evaluation」というリストが管理されており、現在米国でNIAPの認定を受けたCommon Criteria Testing Laboratory(CCTL)による評価が進行中の製品、およびCCEVSの責任者により製品が正式に受理されて評価が開始されるEvaluation Kickoff Meeting(またはこれに相当するもの)が完了した製品が記載されています。

製品が認証されると、NIAPにより、現在有効な認証を持つ製品がNIAPの「Product Compliant List」に掲載されます。2年が経過した認証製品は、現在の保証維持ポリシーに従って再審査されます。保証維持期限が切れた認証は、NIAPの「Archived Products」リストに移ります。

コモンクライテリアのポータルには、コモンクライテリア承認協定(CCRA)のもとで相互承認可能な認証製品が掲載されています。コモンクライテリアのポータルの認証済み製品のリストには製品が5年間掲載されます。アーカイブ済みの認証製品については、コモンクライテリアのポータルに記録が残ります。

次の表に、現在試験機関で評価中の製品、またはコモンクライテリアに適合しているとして認証された製品を示します。

現在の状況

iOS 15のNIAPによる評価のための試験機関での試験は、進行中です。最新情報については「Products in Evaluation(NIAP)」および「Product Compliant List」を参照してください。

オペレーティングシステム/認証日	スキームID/書類	タイトル/プロテクションプロファイル
オペレーティングシステム: iOS 15 **認証日:** —	**スキームID:** まだ認証されていません **書類:** —	**タイトル:** Apple iOS 15: iPhone **プロテクションプロファイル:** Mobile Device Fundamentals(PPモジュールは確認中)
オペレーティングシステム: iOS 14 **認証日:** 2021/09/01	**スキームID:** 11146 **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** Apple iOS 14: iPhone **プロテクションプロファイル:** Mobile Device Fundamentals、VPN Client module、WLAN Clients PP Module、MDM Agent EP

オペレーティングシステム/認証日	スキームID/書類	タイトル/プロテクションプロファイル
オペレーティングシステム: iOS 13 **認証日:** 2020/11/06	**スキームID:** 11036 **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** iPhoneのApple iOS 13 **プロテクションプロファイル:** Mobile Device Fundamentals、VPN Client module、WLAN Clients EP、MDM Agent EP

アーカイブ済みのiOSのコモンクライテリア認証

以下に示す以前のバージョンのiOSについては、コモンクライテリアの認証を取得済みです。これらは、NIAPのポリシーに従ってNIAPによりアーカイブされます。

オペレーティングシステム/認証日	スキームID/書類	タイトル/プロテクションプロファイル
オペレーティングシステム: iOS 12 **認証日:** 2019/03/14	**スキームID:** 10937 **書類:** セキュリティターゲット ガイド	**タイトル:** iOS 12を搭載したiPhone **プロテクションプロファイル:** Mobile Device Fundamentals、VPN Client module、Wireless LAN client EP、MDM Agent EP
オペレーティングシステム: iOS 11 **認証日:** 2018/07/17	**スキームID:** 10851 **書類:** セキュリティターゲット ガイド	**タイトル:** Apple iOS 11 **プロテクションプロファイル:** Mobile Device Fundamentals、Wireless LAN client EP、MDM Agent EP
オペレーティングシステム: iOS 10 **認証日:** 2017/07/27	**スキームID:** 10782 **書類:** セキュリティターゲット、ガイド	**タイトル:** iPhoneおよびiPadデバイスのiOS 10.2 **プロテクションプロファイル:** Mobile Device Fundamentals、Wireless LAN client EP、MDM Agent EP
オペレーティングシステム: iOS 10 **認証日:** 2017/07/27	**スキームID:** 10792 **書類:** セキュリティターゲット、ガイド	**タイトル:** iPhoneおよびiPadのiOS 10.2VPNクライアント **プロテクションプロファイル:** VPNクライアントPP
オペレーティングシステム: iOS 9 **認証日:** 2016/10/14	**スキームID:** 10725 **書類:** セキュリティターゲット、ガイド	**タイトル:** MDMエージェントを搭載したiOS 9.3.2 **プロテクションプロファイル:** Mobile Device Fundamentals、MDM Agent EP
オペレーティングシステム: iOS 9 **認証日:** 2016/10/13	**スキームID:** 10714 **書類:** セキュリティターゲット、ガイド	**タイトル:** iPhoneおよびiPadのOS VPNクライアント **プロテクションプロファイル:** VPNクライアントPP
オペレーティングシステム: iOS 9 **認証日:** 2016/01/28	**スキームID:** 10695 **書類:** セキュリティターゲット、ガイド	**タイトル:** iOS 9 **プロテクションプロファイル:** Mobile Device Fundamentals

iPadOSのセキュリティ認証

iPadOS認証取得の背景

Appleは、適切なコラボレイティブ・プロテクション・プロファイルとFIPS 140-3セキュリティレベルを利用して、オペレーティングシステムのメジャーリリースごとにAppleオペレーティングシステムの認証取得に積極的に取り組んでいます。適合の認証は、最終公開バージョンに対してのみ実施可能です。

注記: 2019年、iPadデバイス用のオペレーティングシステムはiPadOSとして刷新されました。iPadOS 13.1より前は、iPadOSはiOSという名称でした。

iPadOSの暗号モジュールの認証状況

暗号モジュール認証制度(CMVP)では、暗号モジュールの認証状況を、現在の状況に応じて3つの個別のリストで管理しています:

- CMVPの「Implementation Under Test List」に掲載されるには、試験機関がAppleからテストの実施を請け負う必要があります。
- 試験機関でのテストが完了すると、試験機関からCMVPによる認証が勧告されます。CMVPの手数料が支払われると、モジュールが「Modules in Process (MIP) List」に追加されます。「MIP List」では、CMVPによる認証対応の進捗状況を以下の4段階で示しています:
  - **Review Pending:** CMVPのリソース割り当てを待機中です。
  - **In Review:** CMVPのリソースが認証活動を実施中です。
  - **Coordination:** 見つかった問題を試験機関とCMVPで解決中です。
  - **Finalization:** 認証書の発行に関連する活動と手続き。
- CMVPによる認証後、モジュールは適合証明書を受け、認証済みの暗号モジュールリストに追加されます。これには次のものが含まれます:
  - 認証済みのモジュールはactiveとしてマークされます。
  - 5年が経過すると、モジュールはhistoricalとしてマークされます。
  - 何らかの理由でモジュールの認証書が取り消された場合、モジュールはrevokedとしてマークされます。

2020年、CMVPはFIPS 140-3のベースとして国際規格のISO/IEC 19790を採用しました。

FIPS 140-3の認証

現在の状況

iPadOS 14（2020年）のユーザ空間、カーネル空間、Secure Key Storeは、試験機関でのテストが完了し、試験機関からCMVPへ認証が勧告されています。これらは、「Modules in Process List」に掲載されています。

iPadOS 15（2021年）のユーザ空間、カーネル空間、Secure Key Storeは、試験機関での試験が進行中です。これらは、「Implementation Under Test List」に掲載されています。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** iPadOS 15 **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** iPadOS 15 **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** iPadOS 15と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（A9-A14、M1） **全体的なセキュリティレベル:** 2
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** iPadOS 15と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（A9-A14、M1） **全体的なセキュリティレベル:** 2 **物理的セキュリティレベル:** 3
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** iPadOS 14 **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** iPadOS 14 **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** iPadOS 14と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(A9-A14、M1) **全体的なセキュリティレベル:** 2
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** iPadOS 14と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(A9-A14、M1) **全体的なセキュリティレベル:** 2 **物理的セキュリティレベル:** 3

FIPS 140-2の認証

次の表に、試験機関でFIPS 140-2への適合を現在審査中および審査済みの暗号モジュールを示します。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2019 **認証日:** 2021年3月23日	**認証書:** 3856 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v10.0 for ARM **オペレーティングシステム:** iPadOS 13 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** 2021年3月23日	**認証書:** 3855 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v10.0 for ARM **オペレーティングシステム:** iPadOS 13 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** 2021/02/05	**認証書:** 3811 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Secure Key Store Cryptographic Module v10.0 **オペレーティングシステム:** iPadOS 13と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/23	**認証書:** 3438 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v9.0 for ARM **オペレーティングシステム:** iOS 12 **タイプ:** ソフトウェア **セキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/11	**認証書:** 3433 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v9.0 for ARM **オペレーティングシステム:** iOS 12 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/09/10	**認証書:** 3523 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v9.0 **オペレーティングシステム:** iOS 12と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/09、2018/05/22、2018/07/06	**認証書:** 3148 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v8.0 for ARM **オペレーティングシステム:** iOS 11 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/09、2018/05/17、2018/07/03	**認証書:** 3147 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v8.0 for ARM **オペレーティングシステム:** iOS 11 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2019/09/10	**認証書:** 3223 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v1.0 **オペレーティングシステム:** iOS 11と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2016 **認証日:** 2017/02/01	**認証書:** 2828 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple iOS Corecrypto Kernel Module v7.0 **オペレーティングシステム:** iOS 10 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2016 **認証日:** 2017/02/01	**認証書:** 2827 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple iOS Corecrypto Kernel Module v7.0 **オペレーティングシステム:** iOS 10 **タイプ:** ソフトウェア **セキュリティレベル:** 1

以前のバージョン

5年以上が経過した認証書は、CMVPの履歴リストに掲載されています。以下に示す以前のバージョンのiOSについては、暗号モジュールの認証を取得済みです:

- iOS 9(corecryptoモジュールv6.0)
- iOS 8(corecryptoモジュールv5.0)
- iOS 7(corecryptoモジュールv4.0)
- iOS 6(corecryptoモジュールv3.0)

コモンクライテリア(CC)認証取得の背景

Appleは、オペレーティングシステムのメジャーリリースのたびに、iPadOSの認証取得に積極的に取り組んでいます。認証は、最終公開バージョンに対してのみ実施可能です。

コモンクライテリア(CC)認証の取得状況

NIAPが運営している米国スキームでは、「Products in Evaluation」というリストが管理されており、現在米国でNIAPの認定を受けたCommon Criteria Testing Laboratory(CCTL)による評価が進行中の製品、およびCCEVSの責任者により製品が正式に受理されて評価が開始されるEvaluation Kickoff Meeting(またはこれに相当するもの)が完了した製品が記載されています。

製品が認証されると、NIAPにより、現在有効な認証を持つ製品がNIAPの「Product Compliant List」に掲載されます。2年が経過した認証製品は、現在の保証維持ポリシーに従って再審査されます。保証維持期限が切れた認証は、NIAPの「Archived Products」リストに移ります。

コモンクライテリアのポータルには、コモンクライテリア承認協定(CCRA)のもとで相互承認可能な認証製品が掲載されています。コモンクライテリアのポータルの認証済み製品のリストには製品が5年間掲載されます。アーカイブ済みの認証製品については、コモンクライテリアのポータルに記録が残ります。

次の表に、現在試験機関で評価中の製品、またはコモンクライテリアに適合しているとして認証された製品を示します。

現在の状況

iPadOS 15のNIAPによる評価のための試験機関での試験は、進行中です。最新情報については「Products in Evaluation(NIAP)」および「Product Compliant List」を参照してください。

オペレーティングシステム/認証日	スキームID/書類	タイトル/プロテクションプロファイル
オペレーティングシステム: iPadOS 15 **認証日:** 2019/03/14	**スキームID:** — **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** iOS 12を搭載したiPad **プロテクションプロファイル:** Mobile Device Fundamentals、VPN Client module、Wireless LAN client EP、MDM Agent EP
オペレーティングシステム: iPadOS 14 **認証日:** 2021/09/01	**スキームID:** 11147 **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** Apple iPadOS 14: iPad **プロテクションプロファイル:** Mobile Device Fundamentals、VPN Client module、Wireless LAN client EP、MDM Agent EP
オペレーティングシステム: iPadOS 13 **認証日:** 2020/11/06	**スキームID:** 11036 **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** iPadモバイルデバイスのiPadOS 13 **プロテクションプロファイル:** Mobile Device Fundamentals、VPN Client module、Wireless LAN client EP、MDM Agent EP

以前のバージョン

以下に示す以前のバージョンのiOSについては、コモンクライテリアの認証を取得済みです。これらは、NIAPのポリシーに従ってNIAPによりアーカイブされます。

- iOS 12（スキームID: 10937）
- iOS 11（スキームID: 10851）
- iOS 10（スキームID: 107782、10792）
- iOS 9（スキームID: 10725、10714、10695）

macOSのセキュリティ認証

macOS認証取得の背景

Appleは、適切なコラボレイティブ・プロテクション・プロファイルとFIPS 140-3セキュリティレベルを利用して、オペレーティングシステムのメジャーリリースごとにAppleオペレーティングシステムの認証取得に積極的に取り組んでいます。適合の認証は、最終公開バージョンに対してのみ実施可能です。

macOSの暗号モジュールの認証状況

暗号モジュール認証制度(CMVP)では、暗号モジュールの認証状況を、現在の状況に応じて3つの個別のリストで管理しています:

- CMVPの「Implementation Under Test List」に掲載されるには、試験機関がAppleからテストの実施を請け負う必要があります。
- 試験機関でのテストが完了すると、試験機関からCMVPによる認証が勧告されます。CMVPの手数料が支払われると、モジュールが「Modules in Process(MIP)List」に追加されます。「MIP List」では、CMVPによる認証対応の進捗状況を以下の4段階で示しています:
  - **Review Pending:** CMVPのリソース割り当てを待機中です。
  - **In Review:** CMVPのリソースが認証活動を実施中です。
  - **Coordination:** 見つかった問題を試験機関とCMVPで解決中です。
  - **Finalization:** 認証書の発行に関連する活動と手続き。
- CMVPによる認証後、モジュールは適合証明書を受け、認証済みの暗号モジュールリストに追加されます。これには次のものが含まれます:
  - 認証済みのモジュールはactiveとしてマークされます。
  - 5年が経過すると、モジュールはhistoricalとしてマークされます。
  - 何らかの理由でモジュールの認証書が取り消された場合、モジュールはrevokedとしてマークされます。

2020年、CMVPはFIPS 140-3のベースとして国際規格のISO/IEC 19790を採用しました。

次の表に、Apple Macコンピュータの場合、どの暗号モジュールがどのMacテクノロジーに適用できるかを示します。

暗号モジュール	Appleシリコンを搭載したMacコンピュータ	Apple T2セキュリティチップを搭載したMacコンピュータ	Apple T2セキュリティチップを搭載していないIntelベースのMacコンピュータ
Appleシリコンユーザ空間	✓		
Appleシリコンカーネル	✓		
Intelユーザ空間		✓	✓
Intelカーネル		✓	✓
Secure Key Store	✓	✓	

FIPS 140-3の認証

2020年、AppleはAppleシリコンベースのMacコンピュータをリリースしました。暗号モジュールがAppleシリコンまたはIntelベースのどちらのMacコンピュータに該当するかは、次の表の「モジュール情報」の列に記載されています。

注記: Apple T2セキュリティチップは、多くのIntelベースのMacコンピュータに内蔵されています。T2チップの認証について詳しくは、Apple T2セキュリティチップのセキュリティ認証を参照してください。

macOS sshクライアント

OpenSSHは、選択したFIPS 140-3アルゴリズムにFIPS 140-3認証済みモジュールを使用するように構成できます。組織は、パスワード**FIPS140Mode**を使用してAppleから入手できる署名および公証されたインストーラを実行できます。インストーラはMacに2つのファイルを配置します:

- **fips_ssh_config:** /private/etc/ssh/ssh_config.d/に配置されます
- **fips_sshd_config:** /private/etc/ssh/sshd_config.d/に配置されます

macOSはこれらのファイルを使用して、OpenSSHで使用可能な暗号をNISTによって検証された暗号のみに制限し、OpenSSHクライアントがプラットフォームに提供された認証済み暗号モジュールを使用するようにします。管理者は独自のファイルを作成することもできます。詳しくは、macOS 12.0.1以降の`apple_ssh_and_fips`ページを参照してください。

現在の状況

macOS 11 Big Surのユーザ空間、カーネル空間、Secure Key Storeは、試験機関での試験が完了し、試験機関からCMVPへ認証が勧告されています。これらは、「Modules in Process List」に掲載されています。

macOS 12 Montereyのユーザ空間、カーネル空間、Secure Key Storeは、試験機関での試験が進行中です。これらは、「Implementation Under Test List」に掲載されています。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12.0 **オペレーティングシステム:** Appleシリコン上のmacOS 12 Monterey **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12.0 **オペレーティングシステム:** Appleシリコン上のmacOS 12 Monterey **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12.0 **オペレーティングシステム:** Intel上のmacOS 12 Monterey **環境:** Intel、ユーザ、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12.0 **オペレーティングシステム:** Intel上のmacOS 12 Monterey **環境:** Intel、カーネル、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12.0 **オペレーティングシステム:** Appleシリコン上のmacOS 12 Montereyと共に配布されるsepOS、T2を搭載したIntel上のmacOS 12 Montereyと共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(M1およびT2) **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12.0 **オペレーティングシステム:** Appleシリコン上のmacOS 12 Montereyと共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(M1) **セキュリティレベル:** 2 **物理的セキュリティレベル:** 3
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** Intel上のmacOS 11 Big Sur **環境:** Intel、ユーザ、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** Intel上のmacOS 11 Big Sur **環境:** Intel、カーネル、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** Appleシリコン上のmacOS 11 Big Sur **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** Appleシリコン上のmacOS 11 Big Sur **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** Appleシリコン上のmacOS 11 Big Surと共に配布されるsepOS、Intel上のmacOS 11 Big Surと共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(M1) **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** Appleシリコン上のmacOS 11 Big Surと共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(M1) **セキュリティレベル:** 2 **物理的セキュリティレベル:** 3

FIPS 140-2の認証

次の表に、試験機関でFIPS 140-2への適合を現在審査中および審査済みの暗号モジュールを示します。

macOS 10.15 Catalinaのユーザ空間、カーネル空間、Secure Key Storeは、試験機関でのテストが完了し、試験機関からCMVPへ認証が勧告されています。これらは、「Modules in Process List」に掲載されています。

注記: Apple T2セキュリティチップは、多くのIntelベースのMacコンピュータに内蔵されています。T2チップの認証について詳しくは、Apple T2セキュリティチップのセキュリティ認証を参照してください。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2019 **認証日:** 2021年3月24日	**認証書:** 3859 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Space Module for Intel(ccv10) **オペレーティングシステム:** macOS 10.15 Catalina **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** 2021年3月24日	**認証書:** 3858 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v10.0 for Intel(ccv10) **オペレーティングシステム:** macOS 10.15 Catalina **タイプ:** ソフトウェア **セキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/12	**認証書:** 3402 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v9.0 for Intel **オペレーティングシステム:** macOS 10.14 Mojave **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/12	**認証書:** 3431 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v9.0 for Intel **オペレーティングシステム:** macOS 10.14 Mojave **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/22	**認証書:** 3155 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v8.0 for Intel **オペレーティングシステム:** macOS 10.13 High Sierra **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/22	**認証書:** 3156 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v8.0 for Intel **オペレーティングシステム:** macOS 10.13 High Sierra **タイプ:** ソフトウェア **セキュリティレベル:** 1

以前のバージョン

以下に示す以前のバージョンのOS XおよびmacOSについては、暗号モジュールの認証を取得済みです。5年以上が経過したものは、CMVPの履歴リストに掲載されています:

- macOS 10.12 Sierra
- OS X 10.11 El Capitan
- OS X 10.10 Yosemite
- OS X 10.9 Mavericks
- OS X 10.8 Mountain Lion
- OS X 10.7 Lion
- OS X 10.6 Snow Leopard

コモンクライテリア(CC)認証取得の背景

Appleは、オペレーティングシステムのメジャーリリースのたびに、macOSの認証取得に積極的に取り組んでいます。認証は、最終公開バージョンに対してのみ実施可能です。

コモンクライテリア(CC)認証の取得状況

NIAPが運営している米国スキームでは、「Products in Evaluation」というリストが管理されており、現在米国でNIAPの認定を受けたCommon Criteria Testing Laboratory(CCTL)による評価が進行中の製品、およびCCEVSの責任者により製品が正式に受理されて評価が開始されるEvaluation Kickoff Meeting(またはこれに相当するもの)が完了した製品が記載されています。

製品が認証されると、NIAPにより、現在有効な認証を持つ製品がNIAPの「Product Compliant List」に掲載されます。2年が経過した認証製品は、現在の保証維持ポリシーに従って再審査されます。保証維持期限が切れた認証は、NIAPの「Archived Products」リストに移ります。

コモンクライテリアのポータルには、コモンクライテリア承認協定(CCRA)のもとで相互承認可能な認証製品が掲載されています。コモンクライテリアのポータルの認証済み製品のリストには製品が5年間掲載されます。アーカイブ済みの認証製品については、コモンクライテリアのポータルに記録が残ります。

次の表に、現在試験機関で評価中の製品、またはコモンクライテリアに適合しているとして認証された製品を示します。

現在の状況

汎用オペレーティングシステムおよびディスク全体の暗号化(FDE)(AAおよびEE)のプロテクションプロファイルを使用したNIAPによるmacOS 11およびmacOS 12の認証は、現在進行中です。

最新情報については「Products in Evaluation(NIAP)」および「Product Compliant List」を参照してください。

オペレーティングシステム/認証日	スキームID/書類	タイトル/プロテクションプロファイル
オペレーティングシステム: macOS 12 Monterey **認証日:** —	**スキームID:** まだ認証されていません **書類:** —	**タイトル:** macOS 12 Montereyが搭載されているApple FileVault 2 **プロテクションプロファイル:** CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E(確認用PP)
オペレーティングシステム: macOS 12 Monterey **認証日:** —	**スキームID:** まだ認証されていません **書類:** —	**タイトル:** macOS 12 Monterey **プロテクションプロファイル:** PP_OS_V4.21(確認用PP)
オペレーティングシステム: macOS 11 Big Sur **認証日:** —	**スキームID:** まだ認証されていません **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** macOS 11 Big Surが搭載されているApple FileVault 2 **プロテクションプロファイル:** CPP_FDE_AA_V2.0E、CPP_FDE_EE_V2.0E
オペレーティングシステム: macOS 11 Big Sur **認証日:** —	**スキームID:** まだ認証されていません **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** Apple macOS 11 Big Sur **プロテクションプロファイル:** PP_OS_V4.21

オペレーティングシステム/認証日	スキームID/書類	タイトル/プロテクションプロファイル
オペレーティングシステム: macOS 10.15 Catalina **認証日:** 2021年4月29日	**スキームID:** 11078 **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** macOS 10.15 Catalinaを実行しているT2コンピュータ上のApple FileVault 2 **プロテクションプロファイル:** CPP_FDE_AA_V2.0E、CPP_FDE_EE_V2.0E
オペレーティングシステム: macOS 10.15 Catalina **認証日:** 2020/09/23	**スキームID:** 11077 **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** macOS 10.15 Catalina **プロテクションプロファイル:** PP_OS_V4.21

tvOSのセキュリティ認証

tvOS認証取得の背景

Appleは、tvOSの各メジャーリリースに関連する暗号モジュールの認証取得に積極的に取り組んでいます。適合の認証は、最終公開バージョンに対してのみ実施可能です。

tvOSの暗号モジュールの認証状況

暗号モジュール認証制度(CMVP)では、暗号モジュールの認証状況を、現在の状況に応じて3つの個別のリストで管理しています:

- CMVPの「Implementation Under Test List」に掲載されるには、試験機関がAppleからテストの実施を請け負う必要があります。
- 試験機関でのテストが完了すると、試験機関からCMVPによる認証が勧告されます。CMVPの手数料が支払われると、モジュールが「Modules in Process(MIP)List」に追加されます。「MIP List」では、CMVPによる認証対応の進捗状況を以下の4段階で示しています:
  - **Review Pending:** CMVPのリソース割り当てを待機中です。
  - **In Review:** CMVPのリソースが認証活動を実施中です。
  - **Coordination:** 見つかった問題を試験機関とCMVPで解決中です。
  - **Finalization:** 認証書の発行に関連する活動と手続き。
- CMVPによる認証後、モジュールは適合証明書を受け、認証済みの暗号モジュールリストに追加されます。これには次のものが含まれます:
  - 認証済みのモジュールはactiveとしてマークされます。
  - 5年が経過すると、モジュールはhistoricalとしてマークされます。
  - 何らかの理由でモジュールの認証書が取り消された場合、モジュールはrevokedとしてマークされます。

2020年、CMVPはFIPS 140-3のベースとして国際規格のISO/IEC 19790を採用しました。

FIPS 140-3の認証

現在の状況

tvOS 14（2020年）のユーザ空間、カーネル空間、Secure Key Storeは、試験機関でのテストが完了し、試験機関からCMVPへ認証が勧告されています。これらは、「Modules in Process List」に掲載されています。

tvOS 15（2021年）のユーザ空間、カーネル空間、Secure Key Storeは、試験機関での試験が進行中です。これらは、「Implementation Under Test List」に掲載されています。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** tvOS 15 **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** tvOS 15 **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** tvOS 15と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（A10、A12） **全体的なセキュリティレベル:** 2
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** tvOS 14 **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** tvOS 14 **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** tvOS 14と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（A10、A12） **全体的なセキュリティレベル:** 2

FIPS 140-2の認証

次の表に、試験機関でFIPS 140-2への適合を現在審査中および審査済みの暗号モジュールを示します。

tvOS 13(2019年)のユーザ空間、カーネル空間、Secure Key Storeは、試験機関でのテストが完了し、試験機関からCMVPへ認証が勧告されています。これらは、「Modules in Process List」に掲載されています。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2019 **認証日:** 2021年3月23日	**認証書:** 3856 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v10.0 for ARM **オペレーティングシステム:** tvOS 13 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** 2021年3月23日	**認証書:** 3855 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v10.0 for ARM **オペレーティングシステム:** tvOS 13 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** 2021/02/05	**認証書:** 3811 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v10.0 **オペレーティングシステム:** tvOS 13と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/23	**認証書:** 3438 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v9.0 for ARM **オペレーティングシステム:** tvOS 12 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/11	**認証書:** 3433 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v9.0 for ARM **オペレーティングシステム:** tvOS 12 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/09/10	**認証書:** 3523 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v9.0 **オペレーティングシステム:** tvOS 12と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/09、2018/05/22、2018/07/06	**認証書:** 3148 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v8.0 for ARM **オペレーティングシステム:** tvOS 11 **タイプ:** ソフトウェア **セキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/09、2018/05/17、2018/07/03	**認証書:** 3147 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v8.0 for ARM **オペレーティングシステム:** tvOS 11 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2019/09/10	**認証書:** 3223 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v1.0 **オペレーティングシステム:** tvOS 11と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2

watchOSのセキュリティ認証

watchOS認証取得の背景

Appleは、watchOSの各メジャーリリースに関連する暗号モジュールの認証取得に積極的に取り組んでいます。適合の認証は、最終公開バージョンに対してのみ実施可能です。

watchOSの暗号モジュールの認証状況

暗号モジュール認証制度(CMVP)では、暗号モジュールの認証状況を、現在の状況に応じて3つの個別のリストで管理しています:

- CMVPの「Implementation Under Test List」に掲載されるには、試験機関がAppleからテストの実施を請け負う必要があります。
- 試験機関でのテストが完了すると、試験機関からCMVPによる認証が勧告されます。CMVPの手数料が支払われると、モジュールが「Modules in Process(MIP)List」に追加されます。「MIP List」では、CMVPによる認証対応の進捗状況を以下の4段階で示しています:
  - **Review Pending:** CMVPのリソース割り当てを待機中です。
  - **In Review:** CMVPのリソースが認証活動を実施中です。
  - **Coordination:** 見つかった問題を試験機関とCMVPで解決中です。
  - **Finalization:** 認証書の発行に関連する活動と手続き。
- CMVPによる認証後、モジュールは適合証明書を受け、認証済みの暗号モジュールリストに追加されます。これには次のものが含まれます:
  - 認証済みのモジュールはactiveとしてマークされます。
  - 5年が経過すると、モジュールはhistoricalとしてマークされます。
  - 何らかの理由でモジュールの認証書が取り消された場合、モジュールはrevokedとしてマークされます。

2020年、CMVPはFIPS 140-3のベースとして国際規格のISO/IEC 19790を採用しました。

FIPS 140-3の認証

現在の状況

watchOS 7（2020年）のユーザ空間、カーネル空間、Secure Key Storeは、試験機関でのテストが完了し、試験機関からCMVPへ認証が勧告されています。これらは、「Modules in Process List」に掲載されています。

watchOS 8（2021年）のユーザ空間、カーネル空間、Secure Key Storeは、試験機関での試験が進行中です。これらは、「Implementation Under Test List」に掲載されています。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** watchOS 8 **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** watchOS 8 **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** watchOS 8と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（S3、S4、S5、S6） **全体的なセキュリティレベル:** 2
オペレーティングシステムのリリース日: 2021 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v12 **オペレーティングシステム:** watchOS 8と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア（S6） **全体的なセキュリティレベル:** 2 **物理的セキュリティレベル:** 3
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** watchOS 7 **環境:** Appleシリコン、ユーザ、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** watchOS 7 **環境:** Appleシリコン、カーネル、ソフトウェア **タイプ:** ソフトウェア **全体的なセキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** watchOS 7と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(S3、S4、S5、S6) **全体的なセキュリティレベル:** 2
オペレーティングシステムのリリース日: 2020 **認証日:** —	**認証書:** まだ認証されていません **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Module v11.1 **オペレーティングシステム:** watchOS 7と共に配布されるsepOS **環境:** Appleシリコン、Secure Key Store、ハードウェア **タイプ:** ハードウェア(S6) **全体的なセキュリティレベル:** 2 **物理的セキュリティレベル:** 3

FIPS 140-2の認証

次の表に、試験機関でFIPS 140-2への適合を現在審査中および審査済みの暗号モジュールを示します。

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2019 **認証日:** —	**認証書:** 3856 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v10.0 for ARM **オペレーティングシステム:** watchOS 6 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** —	**認証書:** 3855 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v10.0 for ARM **オペレーティングシステム:** watchOS 6 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2019 **認証日:** 2021/02/05	**認証書:** 3811 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v10.0 **オペレーティングシステム:** watchOS 6と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/23	**認証書:** 3438 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v9.0 for ARM **オペレーティングシステム:** watchOS 5 **タイプ:** ソフトウェア **セキュリティレベル:** 1

日付	認証書/書類	モジュール情報
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/04/11	**認証書:** 3433 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v9.0 for ARM **オペレーティングシステム:** watchOS 5 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2018 **認証日:** 2019/09/10	**認証書:** 3523 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v9.0 **オペレーティングシステム:** watchOS 5と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/09、2018/05/22、2018/07/06	**認証書:** 3148 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto User Module v8.0 for ARM **オペレーティングシステム:** watchOS 4 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2018/03/09、2018/05/17、2018/07/03	**認証書:** 3147 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Corecrypto Kernel Module v8.0 for ARM **オペレーティングシステム:** watchOS 4 **タイプ:** ソフトウェア **セキュリティレベル:** 1
オペレーティングシステムのリリース日: 2017 **認証日:** 2019/09/10	**認証書:** 3223 **書類:** 認証書 セキュリティポリシー Crypto Officerガイド	**タイトル:** Apple Secure Key Store Cryptographic Module v1.0 **オペレーティングシステム:** watchOS 4と共に配布されるsepOS **タイプ:** ハードウェア **セキュリティレベル:** 2

ソフトウェアのセキュリティ認証

Appleのソフトウェアのセキュリティ認証の概要

Appleは、sepOSおよびT2ファームウェアについて、米国連邦情報処理規格（FIPS）140-2/-3認証証明書およびその他の証明書を取得し、維持しています。Appleでは、該当する複数のプラットフォームに広く適用される**認証構成要素**から取り組みを始めています。構成要素の1つ目は、ソフトウェアおよびハードウェアの暗号モジュールをAppleが開発するオペレーティングシステム内に展開するために使用されるcorecryptoの認証です。構成要素の2つ目は、多くのAppleデバイスに内蔵されているSecure Enclaveの認証です。3つ目は、Touch IDを搭載したAppleデバイスとFace IDを搭載したデバイスに採用されているSecure Element（SE）の認証です。これらのハードウェア認証構成要素が、より広範なプラットフォームセキュリティ認証の基礎となります。

製品の認証：（コモンクライテリアISO/IEC 15408）

コモンクライテリア（ISO/IEC 15408）は、多くの組織でIT製品のセキュリティ評価を実施するための基礎として使用されている標準規格です。

国際的なコモンクライテリア承認協定（CCRA）のもとで相互承認されている認証については、コモンクライテリアのポータルサイトを参照してください。コモンクライテリアの規格は、CCRA外でも国や私的機関の認定スキームに使用されることがあります。欧州では、SOG-IS協定およびCCRAのもとで相互承認が管理されています。

コモンクライテリア・コミュニティが示している通り、目標は、国際的に承認されている一連のセキュリティ規格によって、明確で信頼できるIT製品のセキュリティ機能の評価を行うことです。コモンクライテリア認証により、製品の機能がセキュリティ規格を満たしているかどうかの独立した評価が与えられるため、IT製品のセキュリティに対する信頼性が向上し、ユーザはより確かな情報に基づいた意思決定を行うことができます。

CCRAを通じて、加盟国は、一貫した信頼レベルにてIT製品の認証を承認することに同意しています。認証前に必要な評価は多岐にわたり、以下のようなものがあります:

- プロテクションプロファイル（PP）
- セキュリティターゲット（ST）
- セキュリティ機能要件（SFR）
- セキュリティ保証要件（SAR）
- 評価保証レベル（EAL）

プロテクションプロファイル（PP）とはデバイスタイプ（モバイルなど）のクラスのセキュリティ要件を指定する書類のことであり、同じクラスに属する異なるIT製品の評価を比較可能にするために使用されます。CCRAの加盟国や加盟地域は、承認されたPPのリストの増大に伴い毎年増え続けています。この協定により、製品のデベロッパは、いずれか1つの認証承認スキーム下で1つの認証を取得すれば、その認証を受け入れるすべての署名国や署名地域で承認されることになります。

セキュリティターゲット(ST)では、IT製品の認証時に評価される**項目**を定義します。STは、STを詳細に評価するために使用される、より具体的な**セキュリティ機能要件(SFR)**に変換されます。

コモンクライテリア(CC)でも**セキュリティ保証要件**を定めています。一般的に認定されている指標の1つが**評価保証レベル(EAL)**です。EALは、よく使われる一連のSARをまとめたもので、比較検証に対応するためにPPおよびSTで指定されることがあります。

過去のPPの多くはアーカイブされており、特定の解決策や環境に焦点を当てて作成された、対象となるPPに置き換えられています。すべてのCCRA加盟国や加盟地域が継続的に相互承認を行えるように協力する中、collaborative Protection Profiles(cPP)の開発と保守のためにinternational Technical Community(iTC)が設立されました。cPPは、はじめからCCRAの署名スキームに対応するように開発されます。CCRA以外のユーザグループや相互承認協定を対象としたPPは、引き続き該当するステークホルダによって開発されます。

Appleは、2015年初旬より、特定のcPPについて、アップデートされたCCRAに基づく認証の取得を目指し始めました。それ以来、AppleはiOSのメジャーリリースごとにコモンクライテリア認証を取得し、新しいPPによって定義されるセキュリティ保証の実現にまで対応範囲を広げてきました。

Appleは、モバイルセキュリティテクノロジーを評価する技術コミュニティで積極的な役割を果たしています。このようなコミュニティには、cPPの開発とアップデートを行うiTCが含まれます。Appleは今後も、現在のPPおよびcPPの評価と、それに基づいた認証を目指していきます。

北米市場のAppleプラットフォームの認証は、通常、国家情報保証パートナーシップ(NIAP)が行います。NIAPは、まだ認証されていない現在評価中のプロジェクトのリストを管理しています。

リストに掲載されている一般的なプラットフォームの認証に加え、一部の市場向けの特定のセキュリティ要件を示すために、その他の認証も発行されています。

Apple製アプリケーションのセキュリティ認証

Apple製アプリケーションの認証取得の背景

Appleは、適切なコモンクライテリア・プロテクションプロファイル(PP)を使用して、Apple製アプリケーションのセキュリティ認証の取得に積極的に取り組んでいます。これらの評価は、Appleが取得しているハードウェアやオペレーティングシステムの認証に基づいています。

2018年に、Appleは、Safariブラウザおよび「連絡先」Appが組み込まれたiOS 11で動作する主要なAppについてアプリケーションのセキュリティ認証の取得を開始しました。Appleでは引き続き、iOS 12、iOS 13およびiPadOS 13.1で動作するAppについて、認証を取得しました。2021年に、macOS 11で動作するAppが対象に追加されます。

暗号モジュールの認証状況

リストに掲載されているApple製Appでは、該当するオペレーティングシステムの暗号モジュールを使用しています。詳しくは、iOSのセキュリティ認証、iPadOSのセキュリティ認証、およびmacOSのセキュリティ認証を参照してください。

コモンクライテリア(CC)認証の取得状況

NIAPが運営している米国スキームでは、「Products in Evaluation」というリストが管理されており、現在米国でNIAPの認定を受けたCommon Criteria Testing Laboratory(CCTL)による評価が進行中の製品、およびCCEVSの責任者により製品が正式に受理されて評価が開始されるEvaluation Kickoff Meeting(またはこれに相当するもの)が完了した製品が記載されています。

製品が認証されると、NIAPにより、現在有効な認証を持つ製品がNIAPの「Product Compliant List」に掲載されます。2年が経過した認証製品は、現在の保証維持ポリシーに従って再審査されます。保証維持期限が切れた認証は、NIAPの「Archived Products 」リストに移ります。

コモンクライテリアのポータルには、コモンクライテリア承認協定(CCRA)のもとで相互承認可能な認証製品が掲載されています。コモンクライテリアのポータルの認証済み製品のリストには製品が5年間掲載されます。アーカイブ済みの認証製品については、コモンクライテリアのポータルに記録が残ります。

次の表に、現在試験機関で評価中の製品、またはコモンクライテリアに適合しているとして認証された製品を示します。

現在の状況

- 進行中として公開されているNIAPによる評価は、Products in Evaluation(NIAP)に掲載されています。
- 評価が完了し、認証された製品はNIAPの「Product Compliant List」に掲載されます。

オペレーティングシステム/認証日	スキームID/書類	タイトル/プロテクションプロファイル
オペレーティングシステム: macOS 11 Big Sur **認証日:** —	**スキームID:** まだ認証されていません **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** macOS 11 Big Sur:「連絡先」 **プロテクションプロファイル:** PP for Application SW、EP for Web Browsers

オペレーティングシステム/認証日	スキームID/書類	タイトル/プロテクションプロファイル
オペレーティングシステム: macOS 11 Big Sur **認証日:** —	**スキームID:** まだ認証されていません **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** macOS 11 Big Sur: Safari **プロテクションプロファイル:** PP for Application SW、EP for Web Browsers
オペレーティングシステム: iOS 14、iPadOS 14 **認証日:** 2021/08/20	**スキームID:** 11191 **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** Apple iOS 14およびiPadOS 14: 「連絡先」 **プロテクションプロファイル:** PP for Application SW、EP for Web Browsers
オペレーティングシステム: iOS 14、iPadOS 14 **認証日:** —	**スキームID:** 11192 **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** Apple iOS 14およびiPadOS 14: Safari **プロテクションプロファイル:** PP for Application SW、EP for Web Browsers
オペレーティングシステム: iOS 13、iPadOS 13 **認証日:** 2020/06/05	**スキームID:** 11060 **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** Apple iOS 13およびiPadOS 13: Safari **プロテクションプロファイル:** PP for Application SW、EP for Web Browsers
オペレーティングシステム: iOS 13、iPadOS 13 **認証日:** 2020/06/05	**スキームID:** 11050 **書類:** 認証書 セキュリティターゲット ガイド 認証報告書 保証活動報告書	**タイトル:** Apple iOS 13およびiPadOS 13: 「連絡先」 **プロテクションプロファイル:** PP for Application SW

アーカイブ済みのApple製Appのコモンクライテリア認証

オペレーティングシステム/認証日	スキームID/書類	タイトル/プロテクションプロファイル
オペレーティングシステム: iOS 12 **認証日:** 2019/06/12	**スキームID:** 10960 **書類:** セキュリティターゲット ガイド	**タイトル:** iOS 12 Safari **プロテクションプロファイル:** PP for Application SW、EP for Web Browsers
オペレーティングシステム: iOS 12 **認証日:** 2019/02/28	**スキームID:** 10961 **書類:** セキュリティターゲット ガイド	**タイトル:** iOS 12「連絡先」 **プロテクションプロファイル:** PP for Application SW
オペレーティングシステム: iOS 11 **認証日:** 2018/11/09	**スキームID:** 10916 **書類:** セキュリティターゲット ガイド	**タイトル:** iOS 11 Safari **プロテクションプロファイル:** PP for Application SW、EP for Web Browsers
オペレーティングシステム: iOS 11 **認証日:** 2018/09/13	**スキームID:** 10915 **書類:** セキュリティターゲット ガイド	**タイトル:** iOS 11「連絡先」 **プロテクションプロファイル:** PP for Application SW

Appleのインターネットサービスのセキュリティ認証

AppleはISO/IEC 27001やISO/IEC 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の情報セキュリティとプライバシー保護の実践が自ずと証明されることになります。

ISO/IEC 27001およびISO/IEC 27018は、国際標準化機構(ISO)が策定する情報セキュリティマネジメントシステム(ISMS)の規格群に属しています。AppleのISMSの一環として、ISO/IEC 27001およびISO/IEC 27018の規格で定義されている通り、附属書Aの管理策の要件をすべて適用宣言書に盛り込んでいます。Appleは、認定審査機関による独立した評価を毎年受けています。

ISO/IEC 27001

IISO/IEC 27001は、情報セキュリティマネジメントシステムの国際規格の1つで、組織において情報セキュリティマネジメントシステムを確立し、実装し、維持管理し、継続的に改善していく上で必要となる条件を定めています。ISO/IEC 27001規格では、以下のセキュリティドメインについても定めており、これらはAppleのISO/IEC認証でも網羅しています:

- 情報セキュリティのポリシー
- 情報セキュリティの組織
- 資産の管理
- 人的資源のセキュリティ
- 物理的および環境的セキュリティ
- 通信および運用管理
- アクセス制御
- 情報システムの取得、開発、保守
- 情報セキュリティインシデント管理
- 事業継続マネジメント
- コンプライアンス

ISO/IEC 27018

ISO/IEC 27018は、パブリッククラウド環境における個人を特定できる情報（Personally Identifiable Information）の保護に関する国際的な実務規範です。ISO/IEC 27018規格では、以下のセキュリティドメインについても定めており、これらはAppleのISO/IEC認証でも網羅しています:

- 同意と選択
- 目的の正当性と詳述
- 収集の制限
- データの最小化
- 利用、保持、開示の制限
- 正確性と品質
- 公開性、透明性、通知
- 個人の参加とアクセス
- 説明責任
- 情報セキュリティ
- プライバシーコンプライアンス

ISO/IEC 27001およびISO/IEC 27018が適用されるAppleのサービス

AppleのISO/IEC 27001およびISO/IEC 27018の認証は、以下のサービスに適用されます:

- Apple Business Chat
- Apple Business Manager
- Appleプッシュ通知サービス（APNs）
- Apple School Manager
- Claris Connect
- FaceTime
- FileMaker Cloud
- iCloud
- iMessage
- iWorkサービス
- 管理対象Apple ID
- スクールワーク
- Siri

認証取得

AppleのISO/IEC 27001およびISO/IEC 27018の認証取得については、審査機関の以下のページで確認できます。

Appleの認証を表示するには、British Standards Institution（BSI）のWebサイトのCertificate and Client Directory searchにアクセスし、「Company」検索フィールドに「Apple」と入力し、「Search」ボタンをクリックして、検索結果を選択し認証を表示します。

注記: Appleが製造していない製品に関する情報や、Appleが管理または検証していない個々のWebサイトについては、推奨や承認なしで提供されています。Appleは他社のWebサイトや製品の選択、性能、使用に関しては一切責任を負いません。Appleは他社のWebサイトの正確性や信頼性についてはいかなる表明もいたしません。詳しくは各メーカーや開発元にお問い合わせください。

macOSセキュリティ・コンプライアンス・プロジェクト

macOSセキュリティ・コンプライアンス・プロジェクト(mSCP)は、セキュリティガイドを作成するために、プログラムによるアプローチを提供するオープンソースの取り組みです。これは、アメリカ国立標準技術研究所(NIST)、アメリカ航空宇宙局(NASA)、アメリカ国防情報システム局(DISA)、およびロスアラモス国立研究所(LANL)の連邦運用ITセキュリティスタッフの共同プロジェクトです。プロジェクトは、macOS用にテストおよび検証された一連のコントロールを使用し、プロジェクトでサポートされているセキュリティガイドに対してこれらのコントロールをマッピングします。さらに、テストおよび検証されたアトミックアクション(設定の構成)のライブラリを活用することにより、技術的なセキュリティ制御のカスタマイズされたセキュリティベースラインを簡単に作成するためのリソースとして、このプロジェクトを使用できます。プロジェクトでは、使用されたベースラインに基づいて、カスタマイズされたドキュメント、スクリプト、構成プロファイル、および監査チェックリストが出力されます。

mSCPは、コンプライアンスを達成するために管理およびセキュリティツールと組み合わせて使用される出力コンテンツを生成できます。このプロジェクトの設定の構成は、以下のガイドベースラインをサポートします。

組織	サポートされているベースライン
アメリカ国立標準技術研究所(NIST)の特別刊行物(SP) 800-53、Recommended Security Controls for Federal Information Systems and Organizations、改訂5	800-53 High、800-53 Moderate、800-53 Low
アメリカ国立標準技術研究所(NIST)の特別刊行物(SP) 800-171、Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations、改訂2	800-171
アメリカ国防情報システム局(DISA)「macOS 11 STIG」、Apple「macOS 11 Security Technical Implementation Guide」	STIG
Committee on National Security Systems Instruction(CNSSI)1253、Security Categorization and Control Selection for National Security Systems	1253

追加情報:

- プロジェクト内のすべてのルールを確認するためのベースラインは、こちらで確認できます。
- プロジェクトと使い方については、「macOS Security Compliance Project wiki」を参照してください。
- 使用するプロジェクトを設定するには、以下を参照してください:「Getting to Know the macOS Security Compliance Project, Part 1」および「Getting to Know the macOS Security Compliance Project, Part 2」。
- プロジェクトの開発をサポートすることに興味がある場合は、「contributor guidance」を参照してください。

ドキュメントの改訂履歴

日付	概要
2021年10月27日	アップデートされたトピック: • Secure Enclave Processorのセキュリティ認証 • iOSのセキュリティ認証 • macOSのセキュリティ認証
2021年8月17日	アップデートされたトピック: • Secure Enclave Processorのセキュリティ認証 • Apple T2セキュリティチップのセキュリティ認証 • iOSのセキュリティ認証 • iPadOSのセキュリティ認証 • macOSのセキュリティ認証 • tvOSのセキュリティ認証 • watchOSのセキュリティ認証 • Apple製アプリケーションのセキュリティ認証 • セキュリティ認証 • macOSセキュリティ・コンプライアンス・プロジェクト
2021年4月26日	追加されたトピック: • macOSセキュリティ・コンプライアンス・プロジェクト アップデートされたトピック: • Apple T2セキュリティチップのセキュリティ認証: 新しいFIPS140-2認証、3811 • Secure Enclave Processorのセキュリティ認証: 新しいFIPS140-2認証、3811、および追加の認証の新しい表。 • iOSのセキュリティ認証: 新しいFIPS140-2認証、3811、iOS14スキームID11146の評価 • iPadOSのセキュリティ認証: 新しいFIPS140-2認証、3811、iPadOS14スキームID11147の評価 • macOSのセキュリティ認証: 新しいFIPS140-2認証、3811 • tvOSのセキュリティ認証: 新しいFIPS140-2認証、3811 • watchOSのセキュリティ認証: 新しいFIPS140-2認証、3811 • Apple製アプリケーションのセキュリティ認証: コモンクライテリアのステータスのアップデート、およびアーカイブ済みのコモンクライテリア認証の新しい表。

用語集

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です。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 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です。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。

collaborative Protection Profile（cPP） cPPの開発を担っている専門家集団であるinternational Technical Communityによって開発されたプロテクションプロファイル。

corecrypto 低レベルの暗号プリミティブの実装を提供するライブラリ。corecryptoは、デベロッパ向けのプログラミングインターフェイスを直接提供するものではなく、デベロッパに提供されるAPIを通じて使用されます。corecryptoのソースコードは公開されているため、セキュリティの特徴や正しく機能しているかどうかを確認することができます。

Implementation under Test（IUT） 試験機関によるテスト中の暗号モジュール。

international Technical Community (iTC) コモンクライテリア承認協定（CCRA）の援助下でプロテクションプロファイルまたはコラボレイティブ・プロテクション・プロファイルの開発を行うグループ。

IPsec VPNクライアント プロテクションプロファイルにおいて、物理または仮想ホストプラットフォームとリモート拠点間の安全なIPsec接続を行うクライアント。

Modules in Process（MIP） 暗号モジュール認証制度（CMVP）によって管理されている、現在CMVPによる認証プロセス中の暗号モジュールのリスト。

Secure Element（SE） 多くのAppleデバイスに内蔵されている、Apple Payなどの機能をサポートするシリコンチップ。

Secure Enclave Processor（SEP） System on Chip（SoC）の内部に搭載されているコプロセッサ。

Senior Officials Group Information Systems Security（SOG-IS） 欧州の複数国間における相互承認協定を管理するグループ。

sepOS L4マイクロカーネルのAppleがカスタマイズしたバージョンに基づいたSecure Enclaveファームウェア。

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む集積回路（IC）。

T2 2017年以降の一部のIntelベースのMacコンピュータに搭載されているAppleのセキュリティチップ。

アメリカ国立標準技術研究所（NIST） 計量に関する科学、規格、および技術の推進を行う米国商務省配下の組織。

コモンクライテリア（CC） ITセキュリティ評価の一般的な概念と原則を確立し、評価の一般的なモデルを規定する規格。標準化された言語でのセキュリティ要件の一覧が含まれています。

コモンクライテリア承認協定（CCRA） ISO/IEC 15408シリーズまたはコモンクライテリアの規格に従って発行される認証の国際承認に関するポリシーと要件を確立する相互承認協定。

セキュリティターゲット（ST） 特定製品のセキュリティ問題およびセキュリティ要件を定める文書。

セキュリティレベル（SL） 適用される一連のセキュリティ要件を示す、ISO/IEC 19790で定義されている4段階の全体的なセキュリティレベル。レベル4が最も厳しい。

ディスク全体の暗号化（FDE） ストレージボリューム上のすべてのデータの暗号化。

プロテクションプロファイル（PP） 特定クラスの製品のセキュリティ問題およびセキュリティ要件を定める文書。

モバイルデバイス管理（MDM） 登録したデバイスをユーザ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、ユーザ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。

暗号アルゴリズム認証制度（CAVP） 承認済み（例えば、FIPSによる承認済みやNISTによる勧告済みなど）の暗号アルゴリズムおよび個々のコンポーネントの認証試験を行う、NISTが運営する組織。

暗号モジュール 暗号機能を備えており、記載されている暗号モジュール規格の要件を満たしているハードウェア、ソフトウェア、ファームウェア。

暗号モジュール認証制度（CMVP） FIPS 140-3規格への適合を認証する、米国およびカナダ政府が運営する組織。

国家情報保証パートナーシップ（NIAP） 米国におけるコモンクライテリア規格への遵守、およびNIAP Common Criteria Evaluation and Validation Scheme（CCEVS）の管理を行う米国政府の組織。

情報セキュリティマネジメントシステム（ISMS） 情報やシステムのライフサイクル全体を通じて体系的に情報セキュリティを管理することによって対象範囲の情報やシステムを保護するように設計されたセキュリティプログラムの限界を管理する、情報セキュリティに関する一連のポリシーおよび手順。

適用宣言書（SOA） ISO/IEC 27001認証の裏付けとして作成される、ISMSの範囲内で実装されるセキュリティ制御が記載される文書。

米国連邦情報処理規格（FIPS） 法令により義務付けられる場合、またはサイバーセキュリティに関して連邦政府による強制的な要件がある場合、あるいはその両方の場合にアメリカ国立標準技術研究所（NIST）が策定する文書。

Apple
One Apple Park Way
Cupertino, CA 95014
USA
apple.com

J028-00499-B