macOSのセキュリティ

IT担当者向けの概要

Appleは、macOSプラットフォームの設計段階から安全性について考慮し、ハードウェア、ソフトウェア、サービスを総合してセキュリティを確保する統合型アプローチを採用しています。また、このアプローチによって、Macの設定、導入、管理が容易になっています。macOSには、IT担当者が企業のデータを保護し、安全な企業ネットワーク環境に統合するための主要なセキュリティテクノロジーが組み込まれています。また、Appleは標準化団体と協力し、最新のセキュリティ認証に確実に適合しています。この概要では、このようなセキュリティ関連の機能について、簡単にご説明します。

この文書は、下記のトピックで構成されています。

- **システムのセキュリティ：**macOSの土台となる安全な統合ソフトウェア。
- **暗号化とデータ保護：**デバイスの紛失や盗難時にユーザーのデータを保護するアーキテクチャとデザイン。
- **アプリケーションのセキュリティ：**Macをマルウェアから保護し、アプリケーションを安全に、プラットフォームの完全性を損ねることなく実行するシステム。
- **認証とデジタル署名：**本人確認情報の管理のためにmacOSに搭載されている機能で、スマートカードやS/MIMEといった業界標準テクノロジーに対応。
- **ネットワークのセキュリティ：**安全な認証と転送時の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。
- **デバイスの管理：**Apple製デバイスの管理を可能にし、不正利用を防止し、デバイスの紛失や盗難時にはリモートワイプを実行できるようにする方法。

macOSの導入と管理についての詳しい情報は、macOS導入リファレンス（help.apple.com/deployment/macos/?lang=ja）を参照してください。

この文書に記載されていない、Appleサービスのセキュリティ機能の詳細については、「iOSのセキュリティ」（www.apple.com/jp/business/docs/iOS_Security_iOS_11_Jan2018_ja.pdf）を参照してください。

システムのセキュリティ

macOSシステムのセキュリティは、Macのすべての主要なコンポーネントで、ソフトウェアとハードウェアの両方が保護されるように設計されています。このアーキテクチャは、macOSのセキュリティの中核であり、デバイスの使いやすさを損なうことがありません。

UNIX

オペレーティングシステムの中核であるmacOSカーネルは、Berkeley Software Distribution（BSD）とMachマイクロカーネルをベースにしています。BSDは、基本的なファイルシステムやネットワークサービス、ユーザーとグループの識別スキームなどを提供します。また、BSDはユーザーIDとグループIDに基づいて、ファイルやシステムのリソースへのアクセス制限を行います。

Machは、メモリ管理、スレッド制御、ハードウェア抽象化、プロセス間通信の機能を提供します。Machは、タスクおよびその他のリソースを表すMachポートに対してどのタスクがメッセージを送ることができるかを制御することで、アクセス制限を徹底します。BSDのセキュリティポリシーとMachのアクセス制御は、macOSのセキュリティにとって不可欠の要素であり、ローカルセキュリティを徹底する上で決定的に重要な役割を担っています。

カーネルのセキュリティは、オペレーティングシステム全体のセキュリティを保つための不可欠な要素です。コード署名は、カーネルと他社製のKernel Extension、またAppleが提供するその他のシステムライブラリや実行ファイルを保護します。

ユーザー権限モデル

Macのセキュリティにおける重要な側面の1つに、アクセス権（アクセス権限とも呼ばれます）の付与と拒否があります。アクセス権とは、データへのアクセスやコードの実行など、特定の操作を実行する資格のことです。アクセス権は、フォルダ、サブフォルダ、ファイル、アプリケーションのレベルで付与されます。また、アプリケーションの機能、管理機能に対しても付与されます。アプリケーションやシステムコンポーネントのアクセス権は、デジタル署名によって判定されます。

macOSは、カーネルのMachコンポーネントとBSDコンポーネントも含めて、アクセス権を様々なレベルで制御します。また、ネットワークアプリケーションに関しては、ネットワークプロトコルを使ってアクセス権を制御します。

強制アクセス制御

macOSには、強制アクセス制御と呼ばれる、デベロッパが設定したセキュリティ制限を適用するポリシーも使われており、これは無効にすることができません。このアプローチは、ユーザーがセキュリティポリシーを環境設定で無効にできる任意アクセス制御とは異なります。強制アクセス制御は、ユーザーからは見えませんが、サンドボックス、ペアレンタルコントロール、管理対象の環境設定、Extension、システム整合性保護など、いくつかの重要な機能を実現するための基盤テクノロジーとなっています。

システム整合性保護

OS X 10.11以降には、システム整合性保護と呼ばれるシステムレベルの保護が実装されており、ファイルシステムの特定の重要な場所にあるコンポーネントを読み取り専用にして、悪意のあるコードがコンポーネントの実行や改ざんをできないようにしています。システム整合性保護はコンピュータ固有の設定で、OS X 10.11にアップグレードした後はデフォルトで有効になっています。この設定を無効にすると、物理ストレージデバイスのすべてのパーティションが保護されなくなります。macOSは、システム上で実行されているプロセスすべてにこのセキュリティポリシーを適用します。サンドボックスで実行されているプロセスも、管理者権限で実行されているプロセスも、すべてが対象になります。

ファイルシステム内の読み取り専用領域の詳細については、Appleのサポート記事「Macのシステム整合性保護について」（support.apple.com/ja-jp/HT204899）を参照してください。

Kernel Extension

macOSには、再コンパイルや再リンクすることなく、動的にカーネルに読み込みが可能なKernel Extension機構が備わっています。このKernel Extension（KEXT）によってコードのモジュール性が高まり、動的な読み込みが可能になります。したがって、ハードウェアのデバイスドライバやVPNアプリケーションのような、内部カーネルのインターフェイスにアクセスする必要がある、比較的自己完結型のサービスにふさわしい仕組みとなっています。

Macのセキュリティを高めるため、macOS High Sierraのインストール時、またはその後にインストールされるKernel Extensionは、ユーザーの承認がなければ読み込むことができません。これをユーザー承認型Kernel Extensionの読み込みと呼んでいます。Kernel Extensionはどのユーザーでも承認でき、管理者権限を必要としません。

次の場合、Kernel Extensionに承認は必要ありません。

- macOS High Sierraへのアップグレード前にインストールされていた場合。
- 以前承認されていたExtensionを置き換える場合。
- macOS復元パーティションからの起動時、spctlコマンドを使って、ユーザーの承認なく読み込むことを許可されている場合。
- モバイルデバイス管理（MDM）の設定で読み込みが許可されている場合。macOS High Sierra 10.13.2からは、MDMを使って、ユーザーの承認がなくても読み込みが許可されるKernel Extensionを指定できるようになりました。このオプションを利用するためには、Macがmacos High Sierra 10.13.2を搭載していること、また、Device Enrollment Program（DEP）かユーザー承認型MDM登録によってMDMに登録されていることが必要になります。

Kernel Extensionの詳細については、「macOS High Sierra のカーネル機能拡張の変更点について準備を進める」（support.apple.com/ja-jp/HT208019）を参照してください。

ファームウェアのパスワード

macOSは、特定のシステムのファームウェア設定に予期しない改変が加えられることを防ぐためのパスワードの使用をサポートしています。ファームウェアのパスワードを使用すると、次のことを防ぐことができます。

- 承認されていないシステムボリュームからの起動
- ブートプロセスの変更（シングルユーザーモードでのブートなど）
- macOS復元に対する不正アクセス
- Thunderboltなどのインターフェイスを通して行うダイレクトメモリアクセス（DMA）
- ターゲットディスクモードの使用（DMAが必要）

注：iMac ProのApple T2チップの場合、ユーザーがMacに物理的にアクセスできたとしても、ファームウェアのパスワードはリセットできないようになっています。Apple T2チップを搭載していないMacの場合、ユーザーがMac内部に物理的にアクセスできないようにする別の手立てが必要になります。

インターネット復元

Macコンピュータは、内蔵の復元システムから起動できない場合、自動的にインターネット経由でmacOS復元による起動を試みます。この場合、起動画面にはAppleのロゴの代わりに回転する地球儀が表示されます。インターネット復元を使うと、最新バージョンのmacOSまたはMacに同梱されていたバージョンを再インストールできます。

macOSのアップデートは、App Storeから配信され、macOSインストーラによって実行されます。インストールの前に、コード署名によってインストーラとパッケージの完全性と真正性が検証されます。これと同様に、インターネット復元サービスも、Macに同梱されていたオペレーティングシステムをインストールするための信頼されたインストール元となります。

macOS復元の詳細については、Appleのサポート記事「macOS復元について」（support.apple.com/ja-jp/HT201314）を参照してください。

暗号化とデータ保護

Apple File System

Apple File System（APFS）は、macOS、iOS、tvOS、watchOSのための最新のファイルシステムです。フラッシュ／SSDストレージ向けに最適化されており、強力な暗号化、メタデータのコピーオンライト、空き領域の共有、ファイルとディレクトリのクローニング、スナップショット、高速なディレクトリサイズの表示、Atomic Safe-Saveプリミティブといった機能を備え、ファイルシステム基盤の向上が図られています。また、独自のコピーオンライト方式を採用しており、データの信頼性は確保しつつ、I/Oコアレッシングを利用してパフォーマンスを最大限に引き出しています。

APFSは、ディスク領域をオンデマンドで割り当てます。1つのAPFSコンテナに複数のボリュームがある場合、コンテナの空き領域は共有され、必要に応じて領域をどのボリュームにも割り当てることができます。各ボリュームはコンテナの一部のみを使用するので、利用可能領域は、コンテナ全体のサイズからコンテナ内のすべてのボリュームの使用済み容量を差し引いた値になります。

macOS High Sierraの場合、有効なAPFSコンテナには少なくとも以下の3つのボリュームが必要ですが、最初の2つはユーザーからは見えないようになっています。

- プリブートボリューム：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ています。
- 復元ボリューム：復元ディスクが格納されています。
- システムボリューム：macOSとユーザーフォルダが格納されています。

FileVault

すべてのMacには、FileVaultと呼ばれる暗号化機能が搭載されており、Mac内のすべてのデータを安全な状態に保つことができます。FileVaultは、XTS-AES-128暗号化方式を用いて、Mac内のデータを保護します。この保護は、内蔵と外付けの両方のストレージデバイスに適用できます。ユーザーが設定アシスタントでApple IDとパスワードを設定すると、FileVaultを有効にして復旧キーをiCloudに保存するよう提案されます。

FileVaultを有効にすると、ブートプロセスの実行時や、ターゲットディスクモードなどの特殊な起動モードにアクセスする場合に、有効な資格情報の入力を求められます。有効なログイン資格情報または復旧キーがなければ、たとえ物理ドライブが取り外され別のコンピュータに接続されたとしても、ボリューム全体が暗号化されたままなので不正アクセスから守られます。

企業が社内のデータを保護する場合は、IT部門がFileVaultの構成ポリシーを定義し、モバイルデバイス管理（MDM）を使って適用する必要があります。暗号化ボリュームを管理する組織には、団体の復旧キー、個人の復旧キー（MDMに保存して預託することも可能）、両者の組み合わせなど、いくつかの管理オプションが用意されています。MDMでは、キーローテーションをポリシーとして設定することもできます。

暗号化されたディスクイメージ

macOSでは、暗号化されたディスクイメージは、機密書類やその他のファイルの保存または転送に使用される安全なコンテナとして機能します。暗号化された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って作成します。ディスクイメージは、128ビットAESまたは256ビットAESのいずれかの暗号化方式を使って暗号化できます。マウントされているディスクイメージは、Macに接続されているローカルボリュームとして扱われるため、このディスクイメージに保存されているファイルやフォルダは、コピーや移動を行ったり開いたりすることができます。FileVaultと同じように、ディスクイメージの中身はリアルタイムで暗号化および復号されます。暗号化したディスクイメージを使えば、ディスクイメージをリムーバブルメディアに保存する、Eメールに添付して送信する、リモートサーバに保存するといった方法で、書類、ファイル、フォルダを安全にやりとりできます。

ISO 27001／27018認証

Appleは、2017年7月11日付の適用宣言書（Statement of Applicability v2.1）により、製品およびサービス（Apple School Manager、iCloud、iMessage、FaceTime、管理対象Apple ID、iTunes U）をサポートするインフラストラクチャ、開発、運用管理について、情報セキュリティマネジメントシステム（ISMS）のISO 27001認証およびISO 27018認証を取得しました。AppleのISO規格への準拠は、BSI（英国規格協会）により認定されています。ISO 27001およびISO 27018認証の認定書は、BSIのウェブサイトでご覧いただけます。

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

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

暗号認定（FIPS 140-2）

macOSの暗号モジュールは、OS X 10.6以降、リリースするたびに米国連邦情報処理規格（FIPS）140-2レベル1に準拠していることが認定されています。メジャーリリースごとに、AppleはMacオペレーティングシステムのリリース時に再認定のためにCMVPにモジュールを提出しています。このプログラムは、macOSの暗号化サービスと承認済みアルゴリズムを適切に使用するAppleのアプリケーションおよび他社製アプリケーションの暗号演算の完全性を保証するプログラムです。AppleのFIPS 140-2適合認定書は、すべてCMVP Vendorページに掲載されています。CMVPは、暗号モジュールの評価状況を2つの個別のリストに分けて、状況別にcsrc.nist.gov/groups/STM/cmvp/inprocess.html（英語）に掲載しています。

コモンクライテリア認証（ISO 15408）

Appleは、これまでもmacOSのコモンクライテリア認証を取得していますが、今またOperating System Protection Profile（PP_OSv4.1）の認証を受けるため、macOS High Sierraの評価に鋭意取り組んでいるところです。今後も、現在利用可能なCollaborative Protection Profile(cPP)の新しいバージョンやアップデートされたバージョンの評価と、それに基づいた認証を目指していきます。これはInternational Technical Community（iTC）で、主要なモバイルセキュリティテクノロジーを評価するcPPの開発で積極的な役割を果たしてきました。

セキュリティに関する認定書、プログラム、ガイダンス

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

macOSのセキュリティに関する認定、評価、ガイダンスの詳細については、Appleのサポート記事「macOS 製品のセキュリティに関する認定書、評価、ガイダンス」（support.apple.com/ja-jp/HT201159）を参照してください。

アプリケーションのセキュリティ

macOSには、信頼されたアプリケーションのみがインストールされ、マルウェアを寄せ付けないようにするために役立つテクノロジーが組み込まれています。さらに、正規のアプリケーションが改ざんされないように、macOSはアプリケーションのランタイム保護と署名に対して階層型のアプローチを採用しています。

Gatekeeper

インストールできるアプリケーションの配布元を制限するために、macOSはGatekeeperと呼ばれる機能を備えています。Gatekeeperによって、ユーザーや組織はアプリケーションのインストールに必要なセキュリティレベルを設定できます。

最も安全度の高いレベルに設定した場合、ユーザーはApp Storeから署名済みのアプリケーションのみをインストールできます。デフォルトの設定では、ユーザーはApp Storeのアプリケーションと Developer IDの署名があるアプリケーションのみをインストールできます。この署名はアプリケーションがAppleの発行した証明書によって署名されており、それ以降に改変されていないことを示しています。Gatekeeperは、必要であればターミナルコマンドで完全に無効にすることもできます。

さらにGatekeeperでは、アプリケーションを署名のないディスクイメージから直接起動した場合やダウンロード後に自動展開した場所から起動した場合などに、パスのランダム化が行われます。パスのランダム化は、読み取り専用に設定されたファイルシステム中の不特定の場所からアプリケーションを起動することで、アプリケーションが相対パスを使ってコードやコンテンツにアクセスすることを防ぎます。また、この読み取り専用の場所で起動している場合はアプリケーションのセルフアップデートを防ぐこともできます。「Finder」を使ってアプリケーションをアプリケーションフォルダなどに移動すると、パスのランダム化は適用されなくなります。

デフォルトの保護モデルの大きなセキュリティ上の利点は、広い範囲でエコシステムを保護することができる点です。たとえマルウェアの作者がDeveloper IDの署名権限を不正に入手または取得し、それを使ってマルウェアを配布したとしても、Appleはその署名の証明書を即座に取り消すことができます。これにより、マルウェアの拡散を防げます。このような保護の仕組みによって、ほとんどの場合Macに対するマルウェアの拡散は経済モデルとして効果がなくなり、結果としてすべてのユーザーに幅広い保護が提供されます。

アプリケーションをインストールするために、ユーザーはこの設定を一時的に無効にすることもできます。組織は、MDMソリューションを使ってGatekeeperの設定を作成して適用したり、コード署名を評価するmacOSの信頼ポリシーに証明書を追加したりできます。

XProtect

macOSは、パターンに基づいてマルウェアを検出するテクノロジーを内蔵しています。AppleはMacのシステムをマルウェアの感染から守るため新たな感染や新型マルウェアの登場を監視し、システムアップデートとは別に、XProtectのパターン情報の自動更新を実行しています。XProtectは既知のマルウェアを自動的に検知し、インストールをブロックします。

マルウェア削除ツール

macOSには、Macにマルウェアが侵入したとしても感染に対処するテクノロジーが搭載されています。Appleは、Developer IDの無効化や（該当する場合）、XProtectの新しいアップデートを発行するためにエコシステム内のマルウェアの活動を監視するだけでなく、感染したシステムからマルウェアを削除するためのアップデートをmacOSに発行します（システムが自動的にセキュリティアップデートを受け取るように設定されている場合）。マルウェア削除ツールが更新情報を受け取ると、次の再起動後にはマルウェアは削除されています。マルウェア削除ツールによってMacが自動的に再起動されることはありません。

自動セキュリティアップデート

Appleは、XProtectとマルウェア削除ツール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。自動セキュリティアップデートの詳細については、Appleのサポート記事「Mac App Store：自動セキュリティアップデート」（support.apple.com/ja-jp/HT204536）を参照してください。

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、ユーザーのアプリケーション空間から保護されています。App Storeから入手したアプリケーションはサンドボックス化されているため、ほかのアプリケーションによって保存されたデータにはアクセスできません。App Storeからインストールされたアプリケーションがほかのアプリケーションのデータにアクセスする必要がある場合は、macOSが提供するAPIとサービスを利用することによってのみ、アクセスが可能になります。

アプリケーションのコード署名の強制

App Storeのアプリケーションは改ざんや変更が加えられていないことを保証するため、すべてAppleによって署名されています。Appleは、Appleデバイスに付属しているアプリケーションにも署名しています。App Store以外で配布されているアプリケーションは、通常、Apple発行のDeveloper ID証明書を使用して（秘密鍵と組み合わせて）デベロッパが署名し、これによりGatekeeperのデフォルト設定で実行できるようになっています。

App Store以外で入手できるアプリケーションは、通常はAppleが発行したデベロッパ証明書で署名されています。これにより、アプリケーションが正規のもので、改ざんされていないことが確認できます。アプリケーションを社内で開発した場合も、完全性を確認できるようにするためAppleが発行したDeveloper IDによる署名が必要です。

システムに保護されたエンタイトルメントを有効にする強制アクセス制御（MAC）を行うにはコード署名が必要です。例えば、ファイアウォールを通してアクセスする必要があるアプリケーションは、適切なMACエンタイトルメントを付与してコード署名を行う必要があります。

認証とデジタル署名

macOSには、ユーザーの資格情報とデジタルIDを簡単かつ安全に保存するために、キーチェーンなどのツールが装備されています。これらのツールは、スマートカードやS/MIMEといった、認証やデジタル署名のテクノロジーにも対応しています。

キーチェーンのアーキテクチャ

macOSにはキーチェーンと呼ばれるリポジトリが用意されており、ユーザー名とパスワード、デジタルID、暗号化鍵、秘密メモなどを簡単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起動します。キーチェーンを使用すると、各リソースの資格情報の入力が不要になり、資格情報を覚える必要さえなくなります。デフォルトで各Macユーザーにキーチェーンが作成されますが、特定の目的のために別のキーチェーンを作成することもできます。

ユーザーキーチェーンのほか、macOSはいくつかのシステムレベルのキーチェーンを使用して、ネットワーク資格情報や公開鍵インフラストラクチャ（PKI）のIDなど、ユーザーに固有ではない認証アセットを管理しています。そうしたキーチェーンの1つであるシステムルートは変更不可で、インターネット上のPKIのルート認証局（CA）証明書を保存します。これにより、オンラインバンキングやEコマースなどの一般的なタスクが利用しやすくなっています。同様に、社内で用意した認証局（CA）の証明書を管理対象のMacに導入し、社内のサイトやサービスの検証に役立てることができます。

安全な認証フレームワーク

キーチェーンのデータは、アクセス制御リスト（ACL）によって分割され保護されているので、他社製アプリケーションが保存した資格情報に別のIDを持つアプリケーションがアクセスすることはできません（ユーザーが明示的に承認した場合を除く）。このような保護構造により、組織内の幅広いアプリケーションやサービス全体にわたって、Appleデバイスの認証資格情報を保護するメカニズムが実現しています。

Touch ID

Touch IDセンサーを搭載したMacは、指紋を使ってロックを解除できます。Touch IDはパスワードに置き換わるものではなく、パスワードはMacの起動、再起動、またはログアウト後のログイン時に必要です。一方、ログインしている場合、ユーザーはパスワードが求められる場面でTouch IDを使ってすばやく認証ができます。

また、「メモ」アプリケーションのパスワード保護されたメモ、Safariの環境設定の「パスワード」パネル、システム環境設定の様々な設定パネルのロックを、Touch IDを使って解除することができます。ただし、セキュリティ強化のため、システム環境設定の「セキュリティとプライバシー」パネルのロック解除にはTouch IDは使えず、パスワードを入力する必要があります。FileVaultが有効になっている場合は、システム環境設定の「ユーザとグループ」パネルを操作する時もパスワードの入力が必要です。複数のユーザーが同じMacにログインしている場合は、Touch IDを使ってアカウントの切り替えができます。

Touch IDおよびTouch IDを使ったセキュリティの詳細については、Appleのサポート記事「Touch IDの先進のセキュリティテクノロジーについて」（support.apple.com/ja-jp/HT204587）を参照してください。

Apple Watchで自動ロック解除

Apple Watchを使ってMacのロックを自動的に解除することができます。Bluetooth Low Energy（BLE）とピアツーピアWi-Fiテクノロジーによって、Apple Watchはデバイス間の距離が近接していることを確認した後、Macのロックを安全に解除します。この機能を使うには、2ファクタ認証（TFA）を設定したiCloudアカウントが必要です。

このプロトコルやContinuityとHandoff機能の詳細については、「iOSのセキュリティ」（www.apple.com/jp/business/docs/iOS_Security_iOS_11_Jan2018_ja.pdf）を参照してください。

スマートカード

macOS Sierra以降は、個人識別認証（PIV）カードに標準で対応しています。このタイプのカードは、2ファクタ認証やデジタル署名、暗号化の目的で企業や政府機関で広く利用されています。

スマートカードには1つ以上のデジタルIDが含まれており、デジタルIDは公開鍵と秘密鍵のペア、関連付けられた証明書で構成されています。個人識別番号（PIN）でスマートカードのロックを解除すると、認証、暗号化、署名に使われる秘密鍵にアクセスできるようになります。証明書によって、鍵を使用できる用途、関連付けられている属性、およびCAで検証済み（署名済み）かどうかが確認できます。

スマードカードは2ファクタ認証に使用することができます。カードのロックを解除するために必要な2つのファクタは、「持っているもの」（カード）と「知っているもの」（PIN）です。macOS Sierra以降は、スマートカードを使ったログイン画面での認証と、Safariでウェブサイトにアクセスする際のクライアント証明書認証に標準で対応しています。また、鍵ペアを使ったKerberos認証（PKINIT）にも対応し、Kerberos対応サービスへのシングルサインオンを行うことができます。

macOSとスマートカードの導入の詳細については、macOS導入リファレンス（help.apple.com/deployment/macos/?lang=ja#/）を参照してください。

デジタル署名と暗号化

「メール」アプリケーションでは、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。互換性のあるスマートカードのPIVトークンが接続されていると、「メール」はPIVトークン上のデジタル署名証明書および暗号化証明書に含まれるサブジェクトまたはサブジェクトの別名（SAN）からRFC 822準拠（大文字と小文字を区別）のEメールアドレスを自動的に検出します。設定済みのメールアカウントが、接続されたPIVトークン上のデジタル署名証明書または暗号化証明書に含まれるメールアドレスと一致した場合、「メール」の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。「メール」が受信者のメール暗号化証明書を持っている場合、またはMicrosoft Exchangeグローバルアドレス一覧（GAL）で証明書を発見できた場合は、新規メッセージのツールバーにロック解除されたカギのアイコンが表示されます。ロックされたカギのアイコンが表示されている場合は、そのメッセージが受信者の公開鍵で暗号化された状態で送信されることを示しています。

メッセージ単位のS/MIME

macOSはメッセージ単位のS/MIMEをサポートしています。そのため、S/MIMEユーザーはデフォルトで署名と暗号化を常に行うか、個別のメッセージごとに署名と暗号化を行うかを選ぶことができます。

S/MIMEで使用するIDは、構成プロファイルやMDMソリューション、SCEP（Simple Certificate Enrollment Protocol）、Microsoft Active Directory認証局などを使ってAppleデバイスに配信できます。

ネットワークのセキュリティ

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

モバイルユーザーは、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なければなりません。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。macOS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。macOSは、このようなセキュリティ上の目標を達成するために実績のあるテクノロジーを搭載し、Wi-Fiデータネットワーク接続の最新の標準規格に対応しています。

TLS

macOSは、Transport Layer Security（TLS 1.0、TLS 1.1、TLS 1.2）およびDTLSに対応しています。また、AES-128とAES-256の両方をサポートしており、PFS（Perfect Forward Secrecy）に対応した暗号スイートを優先的に使用します。Safari、カレンダー、メール、そのほかのインターネットを使うアプリケーションは、このプロトコルを自動的に使用してデバイスとネットワークサービス間の通信を暗号化します。

高レベルAPI（CFNetworkなど）を使うことで、デベロッパはTLSをアプリケーションに簡単に組み込めるようになる一方、低レベルAPI（SecureTransportなど）を使うことで、きめ細かい制御が可能になります。CFNetworkはSSLv3の使用を許可せず、SafariなどWebKitを使用するアプリケーションはSSLv3接続の確立が禁止されます。

macOS High SierraおよびiOS 11では、ユーザーによって信頼された場合を除き、SHA-1証明書をTLS接続に使えなくなりました。また、2048ビット未満のRSA鍵も使用できなくなっています。RC4対称暗号スイートは、macOS SierraとiOS 10では非推奨となっています。デフォルトでは、SecureTransport APIを使って実装されたTLSクライアントまたはサーバで、RC4暗号スイートが無効になっているため、RC4以外の暗号スイートを利用できない場合は接続できません。セキュリティをさらに向上させるため、RC4を必要とするサービスまたはアプリケーションは、アップグレードして最新の安全な暗号スイートを使えるようにする必要があります。

App Transport Security

App Transport Securityは、デフォルトの接続要件を規定します。
それにより、NSURLConnection、CFURL、またはNSURLSessionの各APIの使用時に、アプリケーションがベストプラクティスに従って安全に接続できるようになります。デフォルトでは、App Transport Securityは暗号化方式の選択肢を、前方秘匿性（Forward Secrecy）を持つ暗号スイートのみに限定しています。具体的には、GCMまたはCBCモードのECDHE_ECDSA_AES、ECDHE_RSA_AESだけが使用可能です。アプリケーションはドメインごとに前方秘匿性要件を無効にすることが可能で、その場合は利用できる暗号化のセットに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SHA-256以上を使って署名された有効な証明書も必要です。

アプリケーションがApp Transport Securityを無効にしている場合を除き、上記の条件を満たさないネットワーク接続は失敗します。証明書が無効な場合は必ず失敗し、接続は確立されません。App Transport Securityは、macOS 10.11以降向けにコンパイルされたアプリケーションに自動的に適用されます。

VPN

仮想プライベートネットワーク（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macOSで使用できるようになります。Macコンピュータは、以下のプロトコルと認証方法をサポートするVPNサーバに接続できます。

- IKEv2/IPSec（共有シークレット、RSA証明書、ECDSA証明書、EAP-MSCHAPv2、またはEAP-TLSによる認証）
- SSL-VPN
- Cisco IPSec（パスワード、RSA SecurID、またはCryptoCardによるユーザー認証、および共有シークレットと証明書によるコンピュータ認証）
- L2TP/IPSec（MS-CHAPV2パスワード、RSA SecurID、またはCryptoCardによるユーザー認証、および共有シークレットによるコンピュータ認証）

他社が提供するVPNソリューションのほかに、macOSは以下もサポートしています。

- **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向けです。どのドメインがVPN接続を必要とするかは、ITポリシーにより、VPN構成プロファイルを使用して指定します。
- **Per-App VPN：**VPN接続をさらに細かく管理します。モバイルデバイス管理（MDM）を使用し、アプリケーションごと、またはSafariの特定のドメインごとに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、ユーザー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。

Wi-Fi

macOSは、WPA2 Enterpriseを含む業界標準のWi-Fi規格に対応しており、企業のワイヤレスネットワークへの認証を用いたアクセスを行うことができます。WPA2 Enterpriseは暗号化方式に128ビットAESを採用しているため、ユーザーがWi-Fiネットワークで情報を送受信する際、高いレベルでデータを保護します。また、802.1Xに対応しているので、Macコンピュータを様々なRADIUS認証環境に組み込むことができます。802.1Xワイヤレス認証方法には、EAP-TLS、EAP-TTLS、EAP-FAST、EAP-AKA、PEAPv0、PEAPv1、LEAPなどがあります。

WPA/WPA2 Enterpriseによる認証は、macOSのログイン画面でも使えるため、ユーザーはログイン時にネットワークへの認証も行うことができます。

macOSの設定アシスタントは、ユーザー名とパスワードを資格情報とし、TTLSまたはPEAPを使って接続する802.1X認証に対応しています。

ファイアウォール

macOSは、ネットワークアクセスやDoS（Denial of Service）攻撃からMacを守るファイアウォールを備えています。ファイアウォールは次のような構成をサポートしています。

- アプリケーションに関係なく、外部からの接続をすべてブロックする
- 内蔵ソフトウェアについては、外部からの接続を自動的に受け入れる
- ダウンロードされた署名付きソフトウェアについては、外部からの接続を自動的に受け入れる
- ユーザーの指定したアプリケーションに対して、アクセスを許可または拒否する
- ICMPプローブやポートスキャンにMacが応答しないようにする

シングルサインオン

macOSは、企業ネットワークへのKerberosを使った認証に対応しています。アプリケーションも、ユーザーがアクセス権を付与されているサービスへの認証にKerberosを使うことができます。Kerberosは、幅広い範囲のネットワークアクティビティに利用することができ、Safariの安全なセッションや、NFS（Network File System）への認証や、他社製アプリケーションで使用することもできます。証明書ベースの認証（PKINIT）にも対応していますが、その場合、アプリケーションはデベロッパAPIを利用する必要があります。

GSS-API SPNEGOトークンとHTTP Negotiateプロトコルは、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windows統合認証システムで利用されます。Kerberosへの対応は、オープンソースのHeimdalプロジェクトをベースにしています。

以下の暗号化方式がサポートされています。

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

チケットビューアでのチケットの取得、Windows Active Directoryドメインへのログイン、コマンドラインツールのkinitを使用してKerberosを構成します。

AirDropのセキュリティ

AirDropをサポートするMacコンピュータは、BLE（Bluetooth Low Energy）とAppleが開発したピアツーピアWi-Fiテクノロジーを使用し、iOS 7以降を搭載したAirDrop対応のiOSデバイスなど、近くのデバイスにワイヤレスでファイルや情報を送信できます。通信にはWi-Fi通信が使われ、インターネット接続やWi-Fiアクセスポイントを使わずに、デバイス間で直接通信を行います。この接続は、TLSで暗号化されています。

AirDropとAirDropのセキュリティ、およびその他のAppleサービスの詳細については、「iOSのセキュリティ」（https://www.apple.com/jp/business/docs/iOS_Security_iOS_11_Jan2018_ja.pdf）の「ネットワークのセキュリティ」セクションを参照してください。

デバイスの管理

macOSは、適用と管理が容易な、柔軟なセキュリティポリシーと構成をサポートしています。このため組織では、BYOD（bring your own device）プログラムの一環として社員が自分で用意したコンピュータを使う場合にも、企業情報を保護し、社員が企業の要件を遵守するよう徹底することが可能です。

また、パスワード保護、構成プロファイル、他社製MDMソリューションといったリソースを利用してデバイスの管理を行い、社員が自分のMacコンピュータ上でアクセスしていたとしても、企業データを安全に保つことが可能です。

パスワード保護

パスワードは、推測や攻撃を困難にするために、文字数が多く、複雑なものにすることが推奨されています。

管理者は、モバイルデバイス管理（MDM）を使って、または構成プロファイルを手動でインストールすることをユーザーに要求することで、複雑なパスコードなどのポリシーを実施することができます。macOSの「パスコードポリシー」ペイロードをインストールするには、管理者パスワードが必要となります。

MDM設定で利用できるそれぞれのポリシーの詳細については、help.apple.com/deployment/mdm/?lang=ja#/mdm4D6A472Aを参照してください。

各ポリシーのデベロッパ向けの説明については、構成プロファイルリファレンス（developer.apple.com/jp/documentation/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html）を参照してください。

構成の適用

構成プロファイルは、管理者がMacコンピュータに構成情報を配布するためのXMLファイルです。ユーザーが構成プロファイルを削除すると、プロファイルによって定義された設定もすべて削除されるようになっています。管理者は、ポリシーをWi-Fiやデータアクセスに関連付けることで、ポリシーの設定を徹底することができます。例えば、Eメールの設定を行うための構成プロファイルでデバイスのパスワードポリシーを指定することもできます。その場合、パスワードが管理者の指定した条件を満たさない限り、ユーザーはメールを使うことができません。

macOSの構成プロファイルには、次のような多数の設定項目があります。

- パスコードポリシー
- デバイスの機能制限（カメラを無効にするなど）
- Wi-FiまたはVPNの設定
- メールまたはExchange Serverの設定
- LDAPディレクトリサービスの設定
- ファイアウォールの設定
- 資格情報とその鍵
- ソフトウェアアップデート

プロファイルの最新の設定項目一覧については、モバイルデバイス管理設定（help.apple.com/deployment/mdm/?lang=ja#/mdm5370d089）を参照してください。

構成プロファイルは、署名と暗号化を施すことで、提供元の検証や、完全性の確保、コンテンツの保護を行うことができます。また、構成プロファイルをMacにロックして、削除を完全に防止したり、パスワードを入力した場合のみ削除可能にしたりすることもできます。MacをMDMソリューションに登録する構成プロファイルも削除できます。ただし、削除すると、管理対象の構成情報、データ、アプリケーションもすべて削除されます。

ユーザーは、Safariでダウンロードした構成プロファイルをインストールすることも、メール添付やMDMソリューションを使ってワイヤレスで受信することもできます。ユーザーがDEPまたはApple School Managerに登録されているMacを設定する場合、MacはMDM登録用のプロファイルを自動的にダウンロードしてインストールします。

MDM（モバイルデバイス管理）

macOSはMDMに対応しているため、企業は、大規模に導入されているMac、iPhone、iPad、Apple TVを安全に設定し、管理することができます。このようなMDMの機能は、構成プロファイル、ワイヤレスでの登録、Appleプッシュ通知サービス（APNs）といった既存のmacOSテクノロジーを基盤にしています。例えば、Appleプッシュ通知サービス（APNs）は、デバイスがMDMサーバとセキュリティ保護された接続で直接通信できるように、デバイスのスリープを解除する目的で使用されます。APNsによって機密情報や専有情報が送信されることはありません。

MDMを使うと、IT部門は、企業環境へのMacコンピュータの登録、ワイヤレスでの設定やアップデート、会社のポリシーを準拠しているかどうかの監視、管理対象のMacコンピュータ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。

デバイスの登録

Apple School ManagerおよびApple Deployment Programの一部であるデバイス登録を利用すると、組織がAppleから直接購入したMacコンピュータ、またはプログラムに参加しているApple正規取扱店から購入したMacコンピュータを、迅速に効率よく導入できます。

組織は、コンピュータをユーザーに渡す前に物理的に触れたり準備したりすることなく、MDMに自動的に登録できます。登録後、管理者はプログラムのウェブサイトにサインインして、お使いのMDMソリューションにプログラムをリンクさせます。その後は、MDMソリューションを使って、購入したコンピュータを自動的に割り当てることができるようになります。Macの登録が完了すると、MDMで指定された構成、制限、または制御が自動的にインストールされます。コンピュータとAppleサーバ間の通信は、すべてHTTPSで暗号化されています。

設定アシスタントの特定のステップを省略し、ユーザー側の設定プロセスをさらに簡略化することもできます。これによりユーザーはデバイスをすぐに使い始めることができます。管理者は、ユーザーがMDMプロファイルをコンピュータから削除できるかどうかを制御することも、はじめからデバイスに制限を設定しておくこともできます。箱から出して起動するとすぐに、コンピュータは組織のMDMソリューションに自動的に登録され、管理設定、アプリケーション、本がすべてインストールされます。デバイス登録は、国や地域によっては利用できない場合があります。

企業向けの詳細情報については、Apple Deployment Programヘルプ（help.apple.com/deployment/business/?lang=ja）をご覧ください。
Apple School Managerに関連する詳細情報については、Apple School Managerヘルプ（help.apple.com/schoolmanager/?lang=ja）をご覧ください。

機能制限

管理者は、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、ユーザーがデバイス上のサービス、機能を利用できないようにすることができます。機能制限は、構成プロファイル中の「機能制限」ペイロードでデバイスに送信されます。機能制限はmacOS、iOS、tvOSデバイスに適用できます。

ITマネージャー向けの利用可能な機能制限の最新リストについては、help.apple.com/deployment/mdm/?lang=ja#/mdm2pHf95672で確認できます。

リモートワイプとリモートロック

Macコンピュータは、管理者またはユーザーがリモートで消去できます。ただし、即時のリモートワイプを実行できるのは、FileVaultが有効になっているMacに対してのみです。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、コンピュータは確認応答を送信し、ワイプを実行します。一方、リモートロックを使うと、MDMが6桁のパスコードをMacに設定し、このパスコードを入力しないとだれもロック解除できない状態にすることができます。

プライバシー

Appleは、プライバシーは基本的人権であると信じています。そのため、すべてのApple製品は可能な限りデバイス上で処理を完結させ、データの収集や利用を制限し、情報の透明性とコントロールを保てるように、最初から強固なセキュリティを土台にして設計されています。

Appleは、アプリケーションが情報を利用する方法と条件や、利用する情報の種類をお客様が決定できるように、製品に対して様々な仕組みやオプションを組み込んでいます。詳細については、www.apple.com/jp/privacy/を参照してください。