iPhone/iPadで医療DXを実現

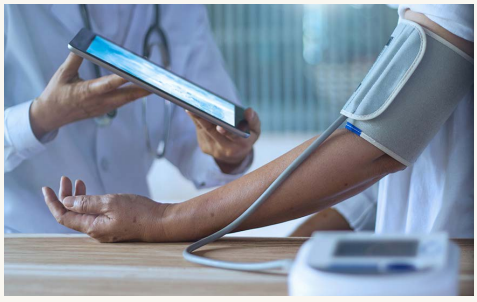
PHS公衆サービスの終了、医師の働き方改革、そして「医療DX令和ビジョン2030」により、医療現場におけるモバイル活用は避けられない流れとなっています。電子カルテ閲覧、院内通話・チャット統合、遠隔診療支援など、業務の中心はスマートフォン/タブレットへと移行しつつあります。しかし求められるのは単なるデバイスの置き換えではなく、セキュリティ・統制・運用効率を同時に満たす基盤です。iPhone/iPadは統合設計による高い安全性と安定性、長時間駆動、集中管理に対応したアーキテクチャを備え、規制対応と生産性向上を両立。「スマートホスピタル」実現に向けた、持続可能なモバイル標準を提示します。

医療現場でのスマートフォン/タブレット導入の現状と課題

［ 訪問先や院外で電子カルテを閲覧できない ］

訪問先や院外から電子カルテを参照したいニーズがあるものの、従来のVPN接続や閉域網を前提とした構成では接続手順が煩雑で通信制約もあり、診療の即時性や業務効率の向上が妨げられています。

［ 便利なアプリやサービスが使えない ］



スマートフォン/タブレット向けの医療アプリやクラウドサービスの活用が期待されているものの、セキュリティや管理面の不安から導入が進まず、現場の利便性向上や情報共有の効率化が阻害されています。

医療現場におけるモバイルデバイス導入に困っていませんか？
iPhone/iPadとJamfで解決できます!

安全性と利便性を両立した「スマートホスピタル」実現のために

現場の医療DXを加速するスマートフォン/タブレット

iPhone/iPad

https://www.apple.com/jp/iphone/
https://www.apple.com/jp/ipad/

＋

iPhone/iPad管理のNo.1ソリューション

Jamf

https://www.jamf.com/ja/resources/press-releases/idc-marketscape/

東京都立多摩総合医療センターでは
iPhoneを1,500台導入しJamfで管理
https://www.tmhp.jp/tama/

詳細はこちらから

講演動画

Jamf事例紹介ページ

なぜ病院はiPhone/iPadを選ぶのか?

AppleのiPhone/iPadは、業務用モバイルデバイスとして国内の病院で広く導入されています。
消費者向けに圧倒的な支持を得ているiPhone/iPadが医療現場でも選ばれ続ける理由を解説します。

1 高性能で堅牢な唯一無二のモバイルデバイス

iPhone/iPadはハードとソフトが一体設計され、Appleシリコンの性能を最大限引き出すようOSやアプリが最適化されているため、日常業務から高負荷アプリまで安定した処理性能を発揮します。また、現在ラインアップされているすべてのiPhoneは16コアのNeural Engineを活用したApple Intelligenceに対応し、オンデバイス中心のAI活用が可能。さらにiPhone/iPadはセキュアブートや顔認証(Face ID)、認証情報保護(Secure Enclave)、データ暗号化、サンドボックス構造などのセキュリティ機能を標準搭載。Apple BusinessとMDM連携によるゼロタッチ展開や遠隔管理にも対応します。

OS一体型セキュリティ設計

iOS/iPadOSはハードと統合設計され、起動時の署名検証やアプリの分離実行などの機能を標準搭載。不正なコード実行や権限の逸脱を抑え、業務アプリが想定外に改変されない運用環境を実現します。

侵害時の横展開防止

各アプリは独立した領域（サンドボックス）で動作し、他のアプリのデータや処理に直接アクセスできません。仮に1つのアプリが不正な挙動を起こしても、院内チャットや通話機能に影響が波及しにくい構造です。

迅速なセキュリティアップデート

Appleが OSとアップデートを一元提供しているため、脆弱性修正や機能更新が対応機種へ一斉配信されます。機種やメーカーの違いによる適用遅延が起きにくく、既知の脆弱性の放置リスクを抑えられます。

オンデバイスAI処理

Apple Intelligenceは、基本的にデバイス内で処理を実行します。AIによる音声の文字起こしや文章の生成·要約などの処理をクラウドに依存せず行えるため、患者情報の外部送信リスクを最小化できます。

2 現場を支える直感的UIと高耐久設計

iPhone/iPadは、世代や職種を問わず扱いやすい直感的なUI設計により、再教育コストを抑えつつ迅速な業務移行を実現します。タッチ応答の速さと滑らかな動作が操作ストレスを軽減し、忙しい現場でも迅速な対応を支えます。高精度マイクと高度な音声処理により、騒音下でも通話や音声入力が安定。さらに、視認性に優れたディスプレイと長時間駆動設計により、長時間の利用でも快適に使えます。こうした設計が、業務効率向上を自然に後押しします。

直感的なUIと統一された操作性

直感的なUIを特徴とするiOS/iPadOSを搭載したiPhone/iPadは、全モデルで操作体系が統一されています。世代による違いが少ないため、学習コストを抑えられ、医師や看護師間でデバイスを共有する際もすぐに利用できます。

高精度マイクと高度な音声処理

iPhone/iPadは複数のマイクとノイズ抑制技術を搭載しており、周囲に環境音がある状況でも音声を明瞭に抽出します。ナースステーションや病棟内でも、音声入力やオンライン会議、ビデオ通話の音質を安定して保ちます。

医療現場に適した耐水·防塵設計

iPhoneは、IP68等級の防水·防塵設計により、水滴や飛沫が付着する環境でも安定して動作します。アルコールによる拭き取りなど日常的な清拭を想定した筐体設計で、液体の侵入による故障リスクを低減します。

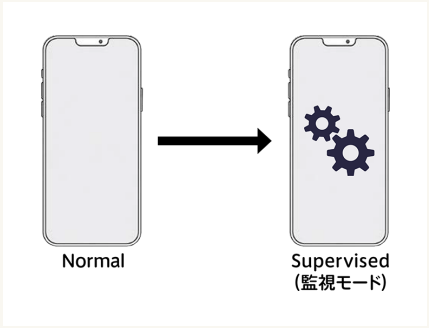
業務を止めない長持ちのバッテリー

iPhone 17は最大30時間、iPad(A16)は最大10時間のビデオ再生に対応。長時間の業務でも安定して使えます。特にiPhoneは、ナースコール対応や緊急連絡が続く状況でもバッテリー切れの不安がなく、業務の中断を防ぎます。

3 デバイス運用を効率化するApple Business

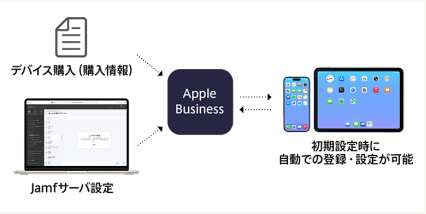
Apple Business（旧：Apple Business Manager）は、組織のiPhone/iPadを管理するためのIT管理者向けのオールインワンプラットフォームです。組織向けのManaged Apple Account（管理対象Appleアカウント）の作成・管理、デバイスの登録・割り当てが行えるほか、初期設定時から自動的に管理下へ組み込む「ゼロタッチ導入」を実現できます。また、一括のアプリケーション購入・配布や、きめ細やかなデバイス管理も可能になります。

組織管理を強化する監視モード



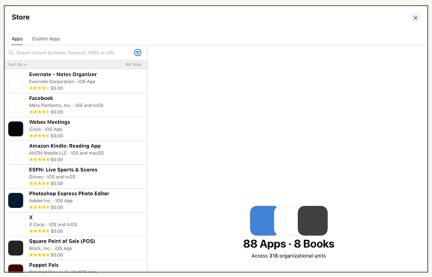
Apple BusinessとMDMを連携すると、iPhone/iPadを「監視モード」に設定でき、組織による高度な管理が可能になります。デバイスの初期化やアクティベーションロックの管理、アプリの一括配布、セキュリティ設定の適用などを一元的に制御できます。

管理者の負担を軽減するゼロタッチ導入



Appleの「自動デバイス登録」（旧DEP）機能を利用すると、Appleまたは正規代理店から購入したiPhone/iPadをApple Businessに簡単に登録し、MDMに紐づけることができます。これにより、デバイスに一切触れることなく初期設定を完了できる「ゼロタッチ導入」が可能です。デバイスを初回起動すると、自動的にAppleのサーバとMDMソリューションに接続され、事前に定義された設定や構成、管理ポリシーが適用されます。

アプリやブックの配布・回収・割り当て

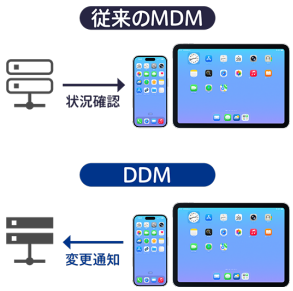


Apple Businessの「Appとブック」（旧VPP）では、Appleの公式ストアから法人単位でアプリやブックを一括購入できます。また、サービストークン（認証キー）をMDMに連携することで、購入したアプリやブックの配布（Apple Account経由、または未使用時はデバイスへ直接配布）や、回収・再割り当てが可能です。

4 組織利用を想定した先進的なセキュリティ機能

Appleは、組織利用を前提としたセキュリティ機能をiPhone/iPad向けに提供しています。デバイスの真正性を証明する仕組みや通信を保護する暗号化技術、共有利用を想定したシェアード対応に加え、高度化するサイバー攻撃に対応するためのデバイス管理機能も継続的に進化しています。これらにより、病院など高いセキュリティと統制が求められる現場においても、信頼性の高い運用をOSレベルで実現します。

自律型管理を実現する「宣言型デバイス管理」

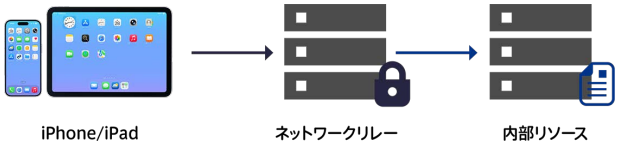


「宣言型デバイス管理」（Declarative Device Management：DDM）は、デバイスが自律的にポリシー準拠状態を維持する次世代の管理モデルです。従来の命令型MDMのように都度指示を送る方式ではなく、あらかじめ定義された目標状態をデバイス側が保持し、逸脱が発生した場合も自律的に修正します。AppleはDDMを将来的なデバイス管理の中核技術と位置づけ、既存MDMと並行して拡張を進めています。これにより、大規模環境でも通信負荷を抑えつつ、リアルタイム性と構成統一を両立した管理が可能になります。

不正デバイス対策「管理対象デバイスの認証」

iOS 16/iPadOS 16.1以降を搭載したiPhone/iPadでは、Secure Enclaveで生成されたデバイス固有鍵を用いてデバイスの正当性を証明し、その結果をAppleのAttestationサーバが検証する「管理対象デバイスの認証」（Managed Device Attestation）が利用できます。検証結果はMDMと連携して活用され、不正なデバイスからのアクセス制御に役立ちます。

VPNに代わる新しい通信方式「ネットワークリレー」



iOS 17/iPadOS 17以降を搭載したiPhone/iPadで利用できる「ネットワークリレー」は、AppleのMASQUE（HTTP/3/QUICベース）技術を活用し、従来のVPNに依存せずに安全な通信経路を確立する仕組みです。アプリ単位でトラフィックを中継できるため、必要な通信のみを効率的に制御でき、効率的かつ柔軟なリモートアクセスを実現します。

複数ユーザで使える「共有iPad」

「共有iPad」は、1台のiPadを複数ユーザで安全に共有できる機能です。ユーザごとのデータは暗号化されて分離管理され、ログイン時に個別の利用環境が呼び出されます。共用環境でも情報の混在を防ぎ、プライバシーと運用効率を両立します。

病院DXのゼロトラスト
iPhone/iPadのセキュリティはJamfで担保

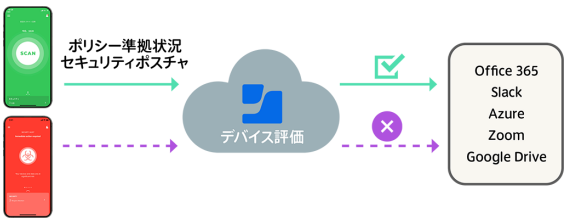
現在の医療現場では、ユーザ・デバイス・アクセスの正当性を常に検証するゼロトラストセキュリティへの転換が求められています。iPhone/iPadの優れたセキュリティに「Jamf for Mobile」を組み合わせることで、ゼロトラストに対応した運用基盤を実現できます。

❶ アクセス制御　認証・認可と医療システムへの安全なアクセス

機関デバイスの証明とクライアント認証

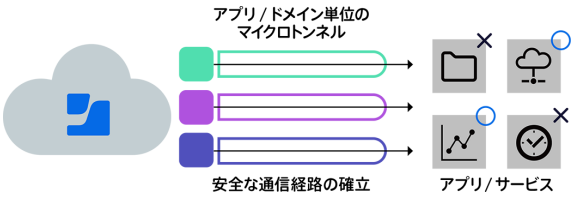
Jamf for Mobileを用いてゼロタッチ導入したiPhone/iPadは、「管理対象デバイスの認証」によって、導入後もそのデバイスの正当性が検証されます。これにより、従来のクライアント証明書に依存せず、なりすましや不正なデバイスの利用を防ぐ、セキュアな認証を実現できます。さらに、パスコードや生体認証、IDaaSによるSSOを組み合わせることで多要素認証を構成でき、ゼロトラストに対応した強固なアクセス制御を実現できます。

“安全なiPhoneだけ”をアクセス可能に



Jamf for Mobileは、iPhone/iPadが組織で管理されたデバイスであることに加え、OSの改ざん（脱獄）の有無やセキュリティアップデートの適用状況などポリシー準拠状況やセキュリティポスチャをもとに、デバイスの安全性を常時評価します。基準を満たさないデバイスは自動的にアクセスを制限されるため、常に安全性が確認されたデバイスのみが業務システムに接続できます。これにより、医療現場においても安心して利用できるセキュアな運用基盤を実現します。

電子カルテや院内へセキュアに接続



Jamf for Mobileを活用すれば、医療従事者は特別な操作なしで院外からでも医療情報システムへ安全に接続できます。通信はアプリケーション/ドメイン単位で制御され、必要なデータのみ暗号化された経路でやりとりされるため、利便性を損なうことなくゼロトラストに基づいた高いセキュリティを確保できます。また、従来のVPN機器や閉域網の構築・運用が不要となり、IT部門の負担を大幅に軽減し、コストを抑えたセキュアなアクセス環境を実現します。

シンプルで簡単な送信元制限への対応

クラウドサービスは、インターネット経由で柔軟に利用できる一方、接続元を制御できない場合、不正デバイスからのアクセスやなりすましのリスクが高まります。そうした課題に対応するため、Jamf for Mobileは、特定の固定IPアドレスを経由した通信経路を提供します。iPhone/iPadからの通信をお客様固有のグローバルIPに集約し、そのIPをアクセス元としてクラウド側で制限することで、未許可デバイスや非所有デバイスからのアクセスを遮断できます。

❷ モバイルEDR　インターネット利用時の安全性確保

危険や不適切なサイトを ブロック

想定外のクラウドサービス利用や不適切コンテンツへのアクセスによる情報漏えいリスクを抑えるには「Webフィルタリング」が有効です。Jamf for Mobileではカテゴリ単位でコンテンツを自動判別し、危険サイトや業務に不要なサイトへのアクセスをブロックすることでリスクを低減します。

フィッシングサイトや 危険なWi-Fi接続対策

スマートフォンやタブレットを狙ったSMSフィッシング攻撃が増加する中、Jamf for MobileはAIによるリアルタイム解析で不正サイトへのアクセスを検知し、自動でブロックします。また、セキュリティが不十分な公衆Wi-Fiやなりすましアクセスポイントなど院外利用時の通信リスクを検知・遮断します。

❸ デバイス管理　安全性と効率性を両立した管理・運用

自動化による デバイス管理の効率化

Jamf for Mobileは「宣言型デバイス管理」に対応しており、OSアップデートの自動実行や時間指定により管理負担を軽減します。また、必要なアプリをすぐに導入できる「Self Service+」や、デバイスの状態に応じて設定を自動適用する「スマートグループ」により手間なく最適な環境を維持できます。

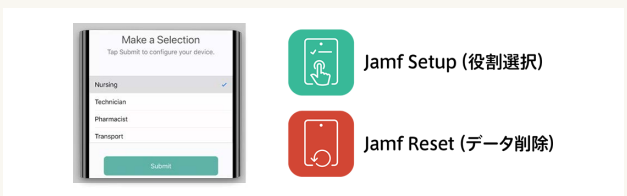
デバイスの利用状況の 見える化

iPhone/iPadの通信時のデータ種別やアクセス先を可視化できるのも、Jamf for Mobileの特長です。通信の利用状況を把握・分析することで、導入サービスの活用状況を確認でき、継続利用の判断にも活用できます。また、不正利用や業務外通信による見えないコストの削減にもつながります。

OSやアプリの脆弱性の 見える化

台数やアプリの増加により病院が保有するデバイス統制が年々難しくなる中、医療情報システムのガイドラインではOSやアプリの脆弱性対策が強く求められています。Jamf for Mobileではこれらの情報をリアルタイムに収集・把握することで、アップデートの自動適用やアクセス制御に活用できます。

共用デバイスの 運用を支える2つのアプリ



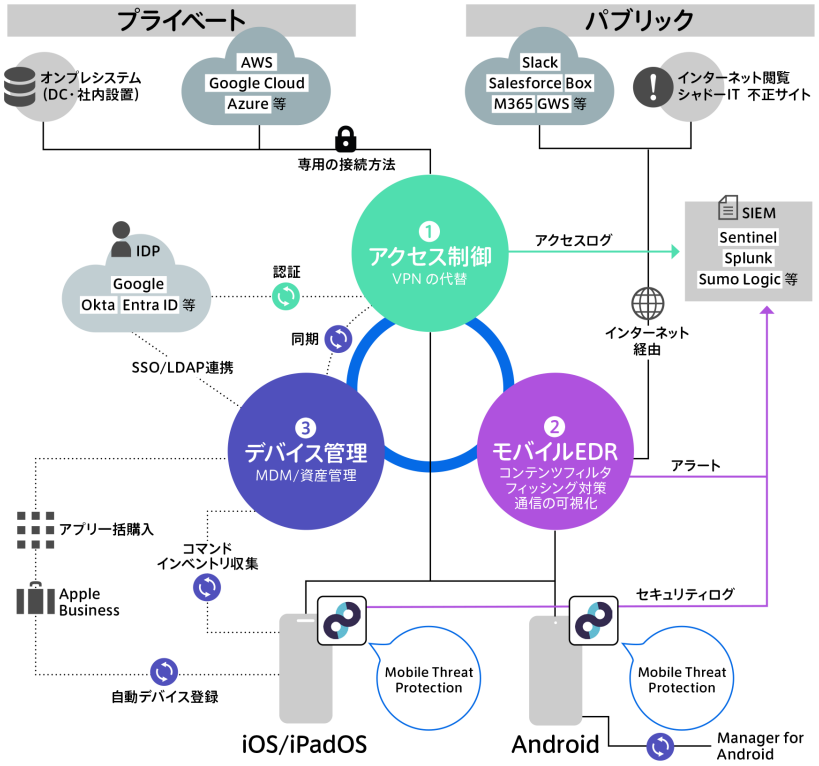
Jamf for Mobileに含まれる「Jamf Setup」と「Jamf Reset」を使えば、複数スタッフでデバイスを共有する場合でも、ユーザ自身で初期設定やデバイスの初期化が可能です。さらに、Microsoft Entra IDと連携することで、ユーザアカウントに基づく認証を強化できます。

「Jamf for Mobile」で実現する iPhone/iPad向けゼロトラストモデル

❶ アクセス制御
- 機関デバイスの認証
- リスクベース認証
- 管理外デバイスからのアクセス防止
- 通信経路の暗号化
- マイクロトンネリング
- 送信元IP固定

❷ モバイルEDR
- Webフィルタリング
- フィッシング対策
- 危険な公衆Wi-Fiの検知
- 不正ソフトウェア対策
- データ通信状況の見える化

❸ デバイス管理
- モバイルデバイス管理
- OS/アプリのバージョン・脆弱性管理
- 共有デバイスの管理統制



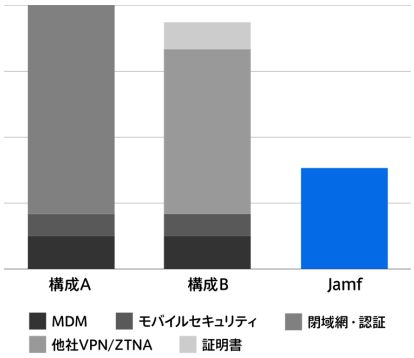
iPhone/iPadとJamfを組み合わせることで、医療情報システムの安全管理ガイドラインに沿ったゼロトラスト構成を実現できます。

Jamfで叶える経済的かつ合理的なiPhone/iPadのゼロトラスト

Jamf for Mobile導入の費用対効果

年間コスト	問い合わせ工数	工事や専用機器
60% 削減	75% 削減	不要

Jamfの導入はiPhone/iPadへの投資効果を最大化し、モバイル全体のコストを最適化します。



Appleのネイティブな技術の活用とJamf for Mobileの導入により、病院のコストと運用負担が軽減されます。

*Jamf Japan調べ
1000台運用時の試算結果
※お客様環境によって結果は異なります。

医療×Jamfに関するFAQはこちらから

jamf

www.jamf.com/ja/

Jamf Japan 合同会社
healthcare_jp@jamf.com