jamf

Jamf + Google – 組織のクラウドネイティブ化を実現するAppleデバイス管理・セキュリティソリューション

デバイス選択制度や柔軟な勤務形態を導入する組織において、IT管理担当者には、エンドユーザの快適性を損なうことなく、**業務効率・セキュリティ・拡張性**を高めることが求められます。

Google Cloud
Google Workspace
chrome enterprise

Appleデバイスの社内導入は、妥協ではなく、戦略的な意思決定として行うべきです。従業員向けにAppleデバイスを支給するのであれば、このプラットフォーム専用のツールが必要になります。Google Workspaceなどの生産性向上ツールは、複数プラットフォームでの運用には有効です。しかし、プラットフォームに関する豊富な専門知識がなければ、デバイスの管理とセキュアな運用は実現できません。

クロスプラットフォーム向けツールやWindows中心のツールでAppleデバイスにも対応しようとすると、以下のような問題や死角が生じ、業務が複雑化しがちです。

1. エンドポイントエージェントが肥大化しパフォーマンスが低下
2. 従来型のVPNは攻撃で狙われる範囲が広く、ユーザエクスペリエンスも低下
3. 可視性が低く、macOS/iOSデバイスを管理しきれない

プラットフォーム専用のツールを用意することが、組織のデバイス活用計画を長期にわたる成功へと導く土台です。Apple向けに最適化されたソリューションへの移行は、業務を支援するだけでなく、Googleエコシステムへの投資の効果も引き出せます。

JamfのAppleファースト型ソリューションは、業界で唯一 Google Workspace / Chrome Enterprise / Google Cloud Identity / Google Security Operationsと緊密に統合可能です。これにより、クラウドファースト型の組織における社内IT部門 / セキュリティ部門のために設計された、合理的なゼロトラスト型エコシステムを構築しています。

GoogleとJamfはあらゆる規模の組織が安全に社内リソースへアクセスし、創造性を発揮し、協調して業務を行えるように連携しています。

JamfはGoogleと連携し、企業のAppleデバイス活用を促進する生産性向上・コラボレーションツールを提供しています。これらのツールはすべて、業務用Appleデバイスを想定したIDベースのゼロトラストシステムで保護されています。

これにより、登録され安全が確認されたデバイスを使用する認可されたユーザのみに、業務用アプリケーションやデータへのアクセスを許可することができます。これらのデバイスは堅牢な管理機能、ネットワーク制御機能、エンドポイントセキュリティ機能で保護されます。すべてのトラフィックがゼロトラストネットワークアクセス（ZTNA）ソリューションで管理されるので、安全性と拡張性に優れたリモートアクセス体制を実現できます。

JamfとGoogleはかねてより、従来のVPNを最新の多層型セキュリティソリューションに置き換えるというビジョンをともに描いてきました。連携することで、現代のハイブリッド型企業のニーズに最適化された、Apple First型のシームレスなゼロトラストソリューションを提供します。

Google Workspaceでセキュアなコラボレーションと生産性向上を実現し、さらにChromeを通じてポリシーベースでMacおよびモバイルデバイス上のブラウザ利用の安全を確保することで、クラス最高レベルの管理・セキュリティ体制でAppleユーザを確実にサポートできます。

Jamfソリューションに Googleが提供するクラウドファースト型の生産性向上ツールとセキュアなブラウザを組み合わせることで、自信を持ってApple製品を中心としたゼロトラスト戦略を導入できます。この統合型のアプローチでは、ユーザとデータを守るだけでなく、勤務場所を問わず従業員の業務の柔軟性、セキュリティ、生産性も高められます。

JamfとGoogleが実現する統合型ゼロトラストセキュリティ

統合の概要	説明	製品ドキュメントまたはMarketplaceの該当ページ	Jamf製品	Google製品
ユーザ/グループ情報を参照するためのセキュアLDAP	ディレクトリ内の組織のユーザに関する情報（名前、メールアドレス、役割など）を参照し、適切なアプリや設定を正しいエンドユーザに届けます。これにより、管理者が手動で情報を入力する必要がなくなります。	**GoogleセキュアLDAPとの統合**	Jamf Pro、Jamf School	Google Workspace、Google Cloud Identity
Googleコンテキストアウェアアクセスとの統合	モバイルデバイス/MacデバイスでJamfが割り出したコンプライアンスステータスをBeyondCorpと共有し、コンテキストアウェアアクセスポリシーの保護対象アプリケーションへのアクセスを制限します。	**Google BeyondCorp Enterprise**	Jamf Pro、Jamf Connect	Google Workspace、Google Cloud Identity、Google Cloud
Chrome Enterprise Core/Premiumの活用	Chrome Enterpriseに搭載されている企業向けの一元管理機能を、Jamf ProおよびJamf SchoolによりGoogle Chrome内で利用できます。	**Jamf ProでのmacOSのブラウザの登録** **Jamf Proでのモバイルデバイスのブラウザの登録**	Jamf Pro、Jamf School	Chrome Enterprise
Cloud Identity 対応のSSO（シングルサインオン）	Jamf Proインスタンス、Jamf macOS Security Cloudポータル、Jamf Security CloudポータルにGoogle認証情報でログインするための管理者向け機能です。	**Google WorkspaceでのSSOの構成**	Jamf Account	Google Workspace、Google Cloud Identity
Mac向けのクラウドベースID	これにより、エンドユーザはGoogleの認証情報を使用してMacにログインすることができます。ユーザエクスペリエンスはChromebookやWindowsでGCPWを使用する場合と同じです。	**Google Identityとの統合**	Jamf Connect	Google Workspace、Google Cloud Identity
Google Security Operations用のJamf Protectパーサー	Jamf ProtectとGoogle Security Operations（SecOps）の統合により、Jamf Protectで収集した詳細なイベントデータ、アラート、統合ログイベントをGoogle SecOpsに送信し記録・分析できます。	**Google Security Operations**	Jamf Protect	Google Security Operations
Google Security Operations用のJamf Proパーサー	Jamf Proのインベントリ情報をGoogle Security Operationsで解析できます。	**Google Security Operations**	Jamf Pro	Google Security Operations
個人所有iOS向けのGoogle Identityによるアカウント駆動型ユーザ登録	ユーザのプライバシーに配慮して、個人所有のモバイルデバイスを管理できます。ユーザは設定アプリからオンボーディングするだけで、Google認証情報を活用しデバイス管理ソリューションに登録し、プロファイルやアプリを受信できます。	**BYOD向けユーザ登録**	Jamf Pro、Jamf School	Google Workspace、Google Cloud Identity

jamf

www.jamf.com/ja/

GoogleとJamfのパートナーシップに関する詳細は、当社ウェブサイトのこちらのページをご覧ください。トライアルでお試しください 。