

スマホでDX! iPhoneの業務活用を促進するための 必須「セキュリティチェックリスト」



iPhoneはビジネス利用に最適なデバイスです。
もし十分に業務に活用できていないなら、それはセキュリティ対策が万全でないからかもしれません。
Appleファーストの管理ソリューションを長年提供してきたJamfが考える、iPhoneを業務活用するために必ず押さえておきたい「セキュリティ対策のポイント」と「ベストな解決策」を紹介します。

iPhoneを業務に活用すべき理由

- 1 iPhoneは従業員が使い慣れている**
2024年1月時点での日本におけるiPhoneのシェアは67%です*。
従業員がプライベートでも使い慣れているiPhoneを仕事でも活用すれば、非常に高い生産性を確保できます。
※ Stats Counter (<https://gs.statcounter.com/>)
- 2 iOS標準のネイティブアプリに多くのビジネス向け機能が搭載されている**
iPhoneに標準搭載されているアプリケーションには、書類のスキャンやテキスト認識、画像認識など、ビジネス向けに使える多くの機能が搭載されています。
- 3 多くの業務はiPhoneで代替できる**
最新のiPhoneは一般的なラップトップPCと変わらない性能を発揮します。また、iPhone向けのApp Storeには23万5,000を超えるビジネスアプリケーションが用意されています*。
※ <https://www.apple.com/jp/business/enterprise/>
- 4 ビジネス向けのアプリが充実している**
勤怠管理を楽にするアプリ、複数バーコードを同時に読み込めるアプリ、iPhoneのカメラを使用して部屋の3Dデザインを作れるアプリなどビジネス課題を解決する多種多様なアプリが充実しています。

iPhoneが
十分活用されていない場合は、
こんな会話が社内で
起きていませんか？



経営者

リモートワーク・DXを
推進するために
iPhoneを
もっと活用しよう!

活用したいとは思っているけれど、
セキュリティのリスクが
ありすぎて無理です!



IT 管理部門

会社全体の方針としてDXを推進していきたい経営者と、セキュリティのリスクを抱えた状態での利活用は難しいという現場の管理部門の葛藤が起きていることが、iPhoneが業務で活用されない最もメジャーな理由です。



iPhoneを業務にもっと活用したいなら
セキュリティ対策が必須です!
チェックリストで確認してみましょう。



業務でスマホ(iPhone)をより活用するために必ず押さえておきたい

✓ セキュリティチェックリスト



① デバイス機能の管理・制御

- ☐ すべての業務用スマートフォンは会社の管理下にありますか？
- ☐ 従業員が勝手にアプリをダウンロードしないようにチェックしていますか？
- ☐ パスコードを設定していますか？



② インターネットトラフィックの管理・制御

- ☐ 従業員による業務用スマートフォンでのインターネット閲覧を管理できていますか？
- ☐ 毎月の社内のモバイルデータ通信量を把握していますか？
- ☐ 外出先から会社のサーバやSaaSへの安全な接続は確立されていますか？



③ デバイスの脅威防御

- ☐ 業務用スマートフォンのマルウェア対策はしていますか？
- ☐ 偽のSMSやメール、サイトに騙されないように対策はしていますか？
- ☐ ゼロデイ攻撃に対応していますか？



④ デバイス状態の可視化

- ☐ OSはいつも最新ですか？ 社内のOSバージョンを確認できる状態ですか？
- ☐ リスクのあるアプリを特定することはできますか？
- ☐ 未管理または改造されたデバイスからの社内情報へのアクセスを防いでいますか？

あなたの会社のiPhoneは大丈夫ですか？
Jamfの製品を導入すればすべてをカバーできます。

デバイスの管理

for Apple

●一般企業向け

jamf | PRO

●SMB 向け

jamf | NOW

●教育機関向け

jamf | SCHOOL

デバイス・ユーザ・データのセキュリティ

for Apple, Android, Windows

●一般企業向け

jamf | CONNECT

- ▶ Cloud-based Identity for macOS
- ▶ Zero Trust Network Access

jamf | PROTECT

- ▶ Endpoint Protection
- ▶ Threat Prevention & Remediation
- ▶ Content Filtering
- ▶ Visibility & Compliance

●政府系機関 & エグゼクティブ向け

Jamf Executive Threat Protection

- ▶ Advanced Detection and Response
- ▶ Destroy Advanced Persistent Threats

●教育機関向け

jamf | SAFE INTERNET

- ▶ Content Filtering and Network Threat Prevention Solution for School

包括ソリューション

ワークフローの改善

●一般企業向け

- Jamf Setup & Reset
- Return to Service
- Jamf Migrate
- Healthcare Workflows

●マーケットプレイス

- 300+ Marketplace Integrations

●教育機関向け

- Jamf Teacher
- Jamf Student
- Jamf Parent

具体的な対策方法は次のページをチェック！





① デバイス機能の管理・制御

- ☐ すべての業務用スマートフォンは会社の管理下にありますか？
- ☐ 従業員が勝手にアプリをダウンロードしないようにチェックしていますか？
- ☐ パスコードを設定していますか？

シンプルでセキュアなAppleデバイス管理 with Jamf Pro



Appleのあらゆるデバイスタイプに対応し、
最新OSへの同日サポートも13年連続で提供

iPhoneは、MDMによって一元管理が可能です。また、ゼロタッチ導入などの仕組みを使えば、管理済みのデバイスのみを従業員に使用してもらえよう体制を統一することもできます。さらに、MDMを使って会社から許可したアプリのみを利用可能にしたり、複雑なパスコード設定の強制や定期的な更新を行ったりすることも可能です。Jamf ProはAppleのあらゆるデバイスタイプに対応し、最新OSへの同日サポートを13年連続^{*}で提供。シンプルかつ安全なデバイス管理を実現します。

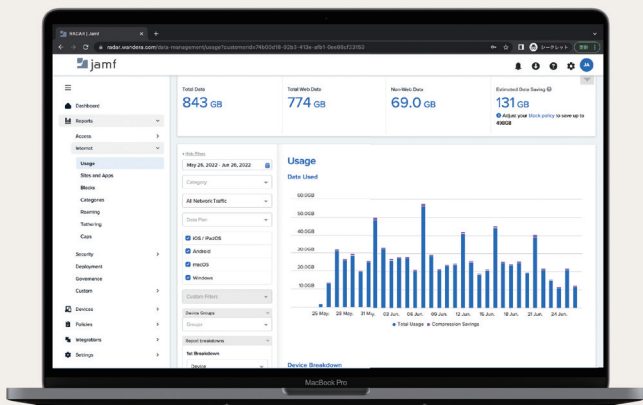
※ 2023年時点



② インターネットトラフィックの管理・制御

- ☐ 従業員による業務用スマートフォンでのインターネット閲覧は管理できていますか？
- ☐ 毎月の社内のモバイルデータ通信量を把握していますか？
- ☐ 外出先から会社のサーバやSaaSへの安全な接続は確立されていますか？

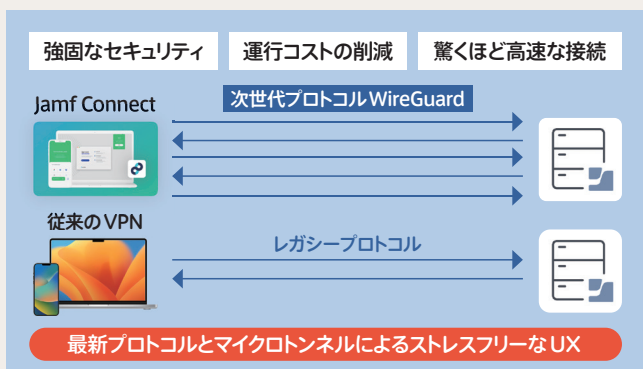
データ通信量のモニタリング with Jamf Protect



ユーザのデータ通信量を
管理者にリアルタイム表示

これまではデバイスの管理・制御を行っていただければ充分でしたが、あらゆる業務がインターネットを介して行われる現在は、インターネット上のセキュリティについても会社が責任を持って担保する必要があります。Jamf Protectを使えば、ネットトラフィックの可視化が可能です。データ通信のモニタリングにより、組織で契約したサービスの利用頻度や、組織が禁止している項目をすり抜けたアクセスなどをチェックでき、監査に役立てられます。また、企業が認めていないストレージサービスなどへのアクセスをブロックすることで、ブラウザとアプリの両方で企業の機密データが漏洩することを防ぐことができます。

ゼロトラストネットワークアクセス with Jamf Connect



次世代のVPNプロトコルで
高速にアクセス可能

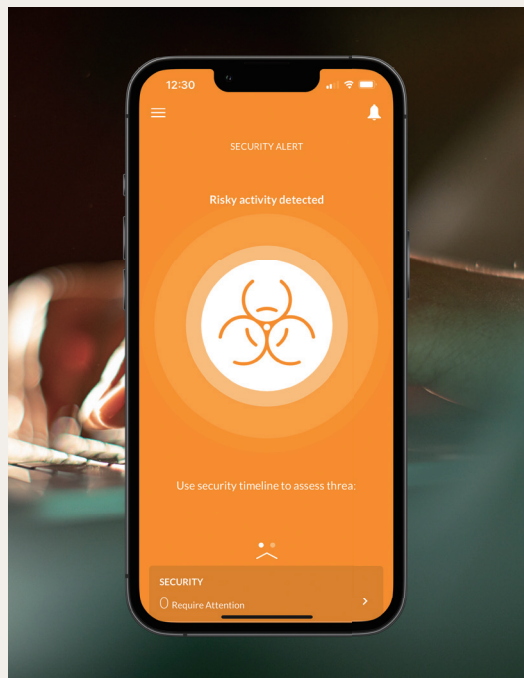
通信そのもののセキュリティを担保することも重要です。Jamfの提供するゼロトラストネットワークアクセスのソリューションは、従来のVPNから比較するとはるかに快適なリモートアクセスを提供します。その鍵となるのが、一般的なVPNプロトコルと比較して約4倍ものスループットを実現する次世代のVPNプロトコル「WireGuard」です。また、Jamf Connectは、端末を再起動した際や5GからWi-Fiにネットワークを切り替えた際なども、VPNの再認証を求めずに安定した接続を続けることができます。「速度も快適でかつ日々の業務の邪魔もしない」といった、まるでVPNを利用していないような感覚で利用いただけます。



③ デバイスの脅威防御

- ☐ 業務用スマートフォンのマルウェア対策はしていますか？
- ☐ 偽のSMSやメール、サイトに騙されないように対策はしていますか？
- ☐ ゼロデイ攻撃に対応していますか？

脅威防御 with Jamf Protect



10人に1人

フィッシングサイトに
アクセスし、かつ情報を
入力している従業員の割合

160%

フィッシング攻撃を受けた
従業員の増加率

93%

HTTPS の
フィッシングドメインの割合

39%

脆弱性を持つ
デバイスを実運用している
組織の割合

データソース : Wandera research data

iPhoneはPCと同等の性能を持つため、
マルウェアやフィッシング攻撃等の脅威にさらされています。

モバイル脅威防御をリードする iOS、iPadOS、Android向けツール

Jamf Protectにはセキュリティの機能が搭載されており、業務用スマートフォンをフィッシングなどのモバイル脅威から守ります。脅威防御を担うこのセキュリティ機能は、iPhoneのみならず iPad や Android 向けにも提供されており、フィッシングサイトやSMSを巧みに利用したスミッシングなどをブロックします。さらに、機械学習エンジン「MI:RIAM」が常に最新のマルウェアやフィッシングサイト等の情報を収集し、従業員をモバイルの脅威から守ります。2023年4月からの1年間で、MI:RIAMが検出したゼロデイのフィッシング攻撃は12万3,000件にもなります。



④ デバイス状態の可視化

- ☐ OSはいつも最新ですか？ 社内のOSバージョンを確認できる状態ですか？
- ☐ リスクのあるアプリを特定することはできますか？
- ☐ 未管理または改造されたデバイスからの社内情報へのアクセスを防いでいますか？

端末情報の可視化 with Jamf Pro



脆弱性の可視化 with Jamf Protect



デバイスの状態を把握し、 リスクのあるiOSやアプリを特定

モバイルデバイス向けの脅威は、デバイスの脆弱性を突いてくることがほとんどです。Jamf Proはデバイスのインベントリ情報をくまなく検出して、その状況をわかりやすいダッシュボードで表示。端末情報の取得・閲覧のみならず、特定の条件に合致するデバイスを動的にグルーピングする機能によって、柔軟な端末管理が可能です。また、Jamf Protectではデバイスだけでなく、OSのバージョンやアプリの脆弱性も検出できます。

※本資料の記載内容は2024年5月現在のものです。



www.jamf.com/ja/

All contents © copyright 2002-2024 Jamf. 無断転載禁止

Jamf Japan 合同会社

東京都港区虎ノ門4丁目1-1 神谷町トラストタワー 25 階

Tel : 050-1790-2200

japan@jamf.com