

JO システム ハードニングガイド

改訂履歴

版数	資料名	更新日	内容
1.0	ハードニングガイド(本文)	2026/9/11	新規発行
1.0	付表 1	2026/9/11	新規発行

免責事項

1.自己責任による実施

本資料に記載された設定変更および対策は、お客様の責任において実施してください。お客様のネットワーク環境やシステム構成によっては、設定変更により通信断、システム停止、または意図しない動作制限が発生する可能性があります。また、本資料の適用判断はお客様に委ねられるものであり、適用によって生じた損害について、当社に故意または重過失がある場合を除き、当社は責任を負いません。

2.事前検証の推奨

設定変更に伴う通信断やシステムの動作変化については、事前にお客様の環境にて十分な検証を行った上で実施してください。

3.完全性の非保証

本資料は、発行時点における一般的なサイバーセキュリティの脅威に対する推奨対策を提示するものであり、あらゆるサイバー攻撃や不正アクセスに対する完全な防御を保証するものではありません。

4.損害に対する責任の制限

当社は、法令により認められる最大限の範囲において、本資料に基づき実施された設定結果、または本資料を利用できなかったことにより生じた直接的、間接的、付随的、結果的、または特別な損害について、一切の責任を負いかねます。

5.情報の更新

サイバーセキュリティの脅威は日々変化します。本資料の内容は予告なく変更されることがあり、常に最新のファームウェアおよびドキュメントを確認することを推奨します。

目次

1. イン트로ダクション	4
1.1 本資料の目的	4
1.2 対象製品	4
1.3 対象読者	4
2. システム内のセキュリティ強化	4
2.1 安全な暗号方式の設定	4
2.2 最新バージョンへのアップデート	5
2.3 正しい日時に設定	7
2.4 利用者変更後の初期化	8
3. システム外のセキュリティ強化	8
3.1 製品の盗難防止対策	8
3.2 システムを構築するネットワーク製品(ルータ等) への対策	9
3.3 使用するスマートフォンの OS を最新バージョンに更新する	10
3.4 セキュリティ製品 (VPN・FW・IPS・IDS 等) のポートフィルタリング設定	10
4. 参考	10

1. イントロダクション

1.1 本資料の目的

当社では製品セキュリティ方針として掲げている、【製品セキュリティポリシー】に則り、インターホンシステムなどのサービスを提供する企業として安全性の高い製品をお客様に提供するとともに利用環境でのセキュリティレベル改善に努めています。

○製品セキュリティポリシー

<https://www.aiphone.co.jp/sustainability/product-security/>

しかし、これらのサービスにおいて、セキュリティレベルを維持するためには利用者の積極的な対応が必要となります。利用者によって安全な利用環境の構築や各製品への設定を適切に行うことでセキュリティレベルの維持および強化することができます。本資料では JO システム の利用者によって行うことができるセキュリティ強化の手順を明記することで、セキュリティレベルの改善を目的としています。

1.2 対象製品

本ハードニングガイドは以下の JO シリーズ製品が対象です。

モニター付親機: JO-1MDW, JO-1MDW V2

モニター付増設親機: JO-1FD

スマートフォンアプリケーション: Intercom app Type B (iOS, Android)

1.3 対象読者

システム利用者

システム管理者

2. システム内のセキュリティ強化

本章では当社製品での設定や管理体制によりセキュリティ強化が見込める方法を示します。

※強化方法に記載の無い製品は対象外となります。

2.1 安全な暗号方式の設定

各端末間やインターネット経由の通信で暗号化を行うこと、また暗号方式は安全なものを使用することはサイバーセキュリティの強化につながります。通信の暗号化をおこなうことで盗聴・改ざん・なりすましといった被害を防ぐことができます。暗号方式を設定する項目がある機能では暗号化の実施および安全な暗号方式を使用するよう設定を行ってください。

●強化方法

■モニター付親機 (JO-1MDW)

Wi-Fi 接続時の暗号化方式を設定することができます。設定する際は本機が対応している暗号化方式のうち、最も安全な「WPA2-PSK (AES)」を選択することを推奨いたします。

◇暗号化方式:None / WEP / WPA-PSK(TKIP/AES) / WPA2-PSK(AES)

◇設定項目:[Settings] ⇒ [Other Settings] ⇒ [Network] ⇒ [Manual Setup] ⇒ [Wi-Fi (Manual Setup)] ⇒ [Encryption]

※設定した暗号化方式は利用している無線ルーターも対応している必要があります。

2.2 最新バージョンへのアップデート

ソフトウェアおよびファームウェアを最新バージョンにしておくことはサイバーセキュリティの強化につながります。当社では、「1.1 本資料の目的」に明記した「情報セキュリティポリシー」に則り、情報セキュリティ対策を行うことで定期的にセキュリティ強化を行っており、ソフトウェアおよびファームウェアのリリースには新しく確認された脆弱性に対する対策がされる場合があります。常に最新バージョンへアップデートするようにしてください。また不正なソフトウェアの混入を防ぐため、ソフトウェアは本資料に記述のダウンロード先から入手するようにしてください。

●強化方法

■モニター付親機

ファームウェアの更新は以下 3 種類の方法で行うことが可能ですが、[ネットワーク経由での自動アップデート]を有効に設定することで、常に最新のファームウェアを維持することができます。

- ・ネットワーク経由での自動アップデート
- ・ネットワーク経由での手動アップデート
- ・SD カードによる手動アップデート

そのため、[ネットワーク経由での自動アップデート]は有効に設定することを推奨しますが、利用用途により、それぞれ以下の手順で定期的なアップデートの実施を行ってください。

◆ネットワーク経由での自動アップデート

自動アップデートを有効に設定しておくことで、最新ファームウェアリリース後、最長 2 日以内に自動でアップデートが開始されます。自動アップデートを有効にする場合は以下のメニューを開き、[Automatic Firmware update]を[Enable]に設定してください。

◇設定項目:[Settings] ⇒ [Other Settings] ⇒ [Station Information] ⇒ [Automatic FW

update]

◆ネットワーク経由での手動アップデート

手動アップデートは「更新通知からの手動アップデート」、[FW 更新確認からの手動アップデート] の2パターンがあります。

◇操作項目：

・更新通知からの手動アップデート

最新ファームウェアリリース後に受信する更新通知から以下の手順で手動アップデートが可能です。

1. MENU 画面から、[(i)] (インフォメーションアイコン) をタップします。
2. 「New firmware available.」の [Check] をタップします。
3. 更新するかどうかを尋ねるメッセージが表示されます。更新するには、[✓] をタップします。
※ファームウェアの更新内容については、モニター付親機に表示された QR コードからウェブサイトアクセスして確認してください。
4. [✓] をタップすると更新が開始されます。
5. 「The firmware has been updated. The station will restart in 5 sec.」と表示されたら更新は完了です。5 秒後に再起動します。

※更新通知を受け取るには事前に以下を設定より[New Firmware Notification]を [Enable]に設定しておく必要があります。

◇設定項目：[Settings] ⇒ [Other Settings] ⇒ [Station Information] ⇒ [Automatic FW update]

・更新確認からの手動アップデート

1. MENU 画面で、[Setting] ⇒ [Other Settings] ⇒ [Station Information] ⇒[Check for FW Update]をタップします。
2. 更新するかどうかを尋ねるメッセージが表示されます。
更新するには、メッセージをよく読んだ後、[✓] をタップします。
3. 更新が完了すると、5 秒後に再起動し、MENU 画面に戻ります。

◆SD カードによる手動アップデート

モニター付親機をネットワークに接続できない場合は SD カードによるアップデートも可能で

す。※microSDHC カードは自身でご用意いただく必要があります。

1. 以下、アイホンのウェブサイトから最新バージョンのファームウェアをダウンロードし、用意した SD カードに保存します。

https://www.aiphone.net/support/software-documents/jo_series/#software

2. ファームウェアを保存した microSDHC カードをモニター付親機に挿入します。
3. microSDHC カードが認識されたら[✓]をタップします
4. モニター付親機にアップデートするかどうかを確認するメッセージが表示されたら、[✓]をタップすると、アップデートが開始されます。
5. 【The firmware has been updated. The station will restart in 5 sec. 】というメッセージが表示されたら、アップデートは完了です。5 秒後に再起動します。

■スマートフォンアプリケーション

スマートフォンアプリケーションのアップデートはインストールした各アプリストアより実施することが可能です。以下、アプリストアの URL に展開していますので、定期的に確認し、最新バージョンへアップデートを行ってください。

◇ソフトウェア・ファームウェアリリース場所

・Intercom App Type B アプリ(iOS 版)

<https://apps.apple.com/jp/app/intercom-app-type-b/id1434675976>

・Intercom App Type B アプリ(Android 版)

<https://play.google.com/store/apps/details?id=jp.co.aiphone.josmartphone&hl=ja>

2.3 正しい日時に設定

正確な日時情報に設定しておくことはサイバーセキュリティにおいて重要です。正しい日時に設定しておくことで過去の通信データを再利用するリプレイ攻撃等、時間のずれを悪用した攻撃を防止することができます。また、セキュリティ侵害時の原因究明においても動作ログなどに正確に日時情報が記録されていれば攻撃の発生日時や経路を特定しやすくなります。

●強化方法

■モニター付親機(JO-1MDW)

インターネット接続時は自動同期されるよう正しい地域のタイムゾーンを設定し、オフライン時は手動で正確な日時を設定してください。

※スマホアプリ連動を行っている場合はすでに自動同期されているため、設定は不要です。

◇設定項目：

タイムゾーン設定:[Settings] ⇒ [Date / Time] ⇒ [Date / Time Format]

手動設定:[Settings] ⇒ [Date / Time] ⇒ [Current Time]

■スマートフォンアプリケーション

スマートフォンの時刻は OS の設定に紐づきます。OS 側の設定に沿って正確な時刻に設定してください。

2.4 利用者変更後の初期化

利用者が変更になった場合、そのまま利用されると新しい利用者に呼出履歴や録画データなどの個人情報を閲覧される可能性があります。利用者が変更となった場合は必ず以下の対応を行うようにしてください。

●強化方法

■モニター付親機

工場出荷時設定へのリセットを行うことで保存されている個人情報の削除が可能です。居住者の交代や親機の譲渡時には、必ず工場出荷時設定へのリセットを実施してください。

◇設定項目:[Settings] ⇒ [Other Settings] ⇒ [Administrator Settings] ⇒ [Factory Reset]

■モニター付増設親機

本機には録画データやネットワーク設定等の個人情報は保存されません。しかし、利用者が変更になる際は、本体底面の「RESET ボタン」を押し、各設定(呼出音量や画面の明るさ等)を工場出荷時のデフォルト状態に戻すことを推奨します。

■スマートフォンアプリケーション

利用しているスマートフォンの機種変更や紛失時には、モニター付親機側から該当する端末の登録削除を確実に行ってください。

◇設定項目:[Settings] ⇒ [Other Settings] ⇒ [Register / Delete apps] ⇒ [Delete Apps]

3. システム外のセキュリティ強化

3.1 製品の盗難防止対策

JO システムで使用するインターホン端末・スマートフォンが第三者に盗まれた場合、内部データが窃取される可能性があります。盗難防止のため可能な限り、以下の対策を行ってください。

◇接続機器の設置

JO シリーズの各製品を壁に設置する場合は付属の接続器具を使用し、取り外しができないようしっかりと固定してください。また、モニター付親機はプライベート空間で利用する製品となります。パブリック空間に設置すると、許可されていない者に利用される可能性があるため。必ずプライベート空間に設置するようにしてください。

◇配線の隠蔽

子機から室内へ繋がる 2 線式配線、解錠用の配線が露出していると、切断や信号操作による妨害を受ける恐れがあります。必ず壁内配線または電線管(配管)を用いて保護してください。

◇画面ロックの設定

使用するスマートフォンは画面ロックを設定し、盗難・紛失時に第三者が「Intercom app Type B」を操作できないようにしてください。また、スマートフォンではアプリ単位でのロック機能も設定することを推奨いたします。

3.2 システムを構築するネットワーク製品(ルーター等) への対策

JO システムではシステムを構築するためにネットワーク製品(ルーター等)を使用していますが、それらネットワーク製品の脆弱性や設定不備により JO システムへサイバー攻撃が行われる可能性があります。これらを防ぐために使用するネットワーク製品のセキュリティ強化を行うことは重要です。以下にセキュリティ強化が見込める対処法をまとめていますので、実施することを推奨いたします。

◇ネットワーク製品への不正アクセスに関する対策

使用するネットワーク製品(ルーター等)が攻撃者からアクセス可能な場所に設置されている場合、ネットワーク製品を経由して JO システムへ不正アクセスされる可能性があります。そのため、ネットワーク製品は許可されているユーザーのみアクセス可能な場所に設置してください。

◇定期的なファームウェア更新

使用するネットワーク製品(ルーター等)について、定期的に最新のファームウェアが提供されていることを確認し、ファームウェア更新を実施することを推奨いたします。

◇初期パラメータの変更

ネットワーク製品に設定されている管理者 ID やパスワード(ルーターの場合は SSID やパスフレーズ)を初期設定のままとしておくことはセキュリティ上、非常に危険です。推測困難で強力な値に変更することでセキュリティ強化が見込めます。

◇暗号化方式の選択

JO システムをルーター経由でインターネット接続している場合、Wi-Fi の暗号化方式についても設定内容の確認が必要です。ルーターによっては暗号方式の初期設定が WEP や WPA 等、脆弱性のある暗号方式に設定されている可能性があります。脆弱な暗号方式に設定されたままの場合、攻撃者によってルーター経由の通信が傍受され、通信内容を盗聴される可能性があります。そのため、脆弱性のある暗号方式が設定されている場合、安全な暗号方式(WPA2-PSK (AES)を推奨)に設定変更することでセキュリティ強化が見込めます。

◇UPnP 機能の無効化

UPnP 機能はネットワークに接続する機器同士の通信を自動化できる便利な機能ですが、セキュリティ上リスクを含む機能でもあります。そのため、不要な場合は利用しているルーターで無効に設定することを推奨いたします。

3.3 使用するスマートフォンの OS を最新バージョンに更新する

使用するスマートフォンの OS を常に最新バージョンに更新することでセキュリティ強度を保つことができます。最新バージョンの OS には過去に発見された脆弱性に対する修正プログラムや最新のセキュリティパッチが含まれており、セキュリティ強度を向上させることが可能です。また、当社スマートフォンアプリケーションのセキュリティ強化にもつながります。そのため、最新バージョンの OS がリリースされた場合はバージョンアップを行うことを推奨いたします。OS バージョンアップはご使用のスマートフォンや OS の実施手順に沿って行ってください。

3.4 セキュリティ製品 (VPN・FW・IPS・IDS 等) のポートフィルタリング設定

VPN、FW、IPS、IDS といったセキュリティ製品には通信ポートのフィルタリング設定をおこなう機能があり、この機能を使用することで攻撃者からの不正アクセスを防ぐことができます。

JO システムでは以下の使用ポート一覧に記載されたポートを使用しているため、必要ポートはアクセスを許可、不要なポートはアクセスを拒否するようフィルタリング設定をすることで JO システムのセキュリティ強化が見込めます。

◇JO 使用ポート一覧

付表 1_使用ポート一覧(JO システム)

上記一覧より使用する機能を明確にし、セキュリティ製品にてフィルタリング設定を行うことを推奨いたします。

4. 参考

詳細な操作方法は、以下の取扱説明書を参照してください。

◇JO システム 取扱説明書

https://www.aiphone.net/support/software-documents/jo_series/

本資料に記載されている「AIPHONE」および各製品名は、アイホン株式会社の商標または登録商標です。

App Store、iOS は Apple Inc.の商標または登録商標です。

Google Play、Android は Google LLC の商標または登録商標です。

その他、記載されている会社名、製品名は各社の商標または登録商標です。