

IP ネットワーク対応インターホン
IX システム IXG 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
1.0	付表2	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. イントロダクション	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	5
2.1 安全な暗号方式の設定	5
2.2 不要なサービスの無効化	6
2.3 最新バージョンへのアップデート	7
2.4 安全なパスワードの設定	9
2.5 正しい日時に設定	12
2.6 権限の分離	13
2.7 権限の適切な失効	15
2.8 TLS 証明書(SSL 証明書)に対するセキュリティ強化	17
2.9 IEEE802.1X 認証方式のセキュリティ強化	18
3. システム外のセキュリティ強化	20
3.1 製品の盗難防止対策	21
3.2 システムを構築するネットワーク製品(スイッチングハブ・ルータ) への対策	21
3.3 使用する PC・スマートフォンの OS を最新バージョンに更新する	22
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	23
4. 参考	23

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処が必要となります。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 IP ネットワーク対応インターホン(IX システム、IXG 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対象製品一覧に記載された IP ネットワーク対応インターホン(IX システム、IXG システム)の製品が対象です。

○対象製品一覧

付表 1_対象製品一覧_(IX システム・IXG システム) 参照

1.3 対象読者

IP ネットワーク対応インターホン(IX システム、IXG システム)を利用する以下の者が対象となります。

○対象者

- ・システム利用者
- ・システム管理者
- ・施工者

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。

また、各セキュリティ強化の対象製品は「1.2 対象製品」に記載している「対象製品一覧」をご確認ください。

【補足】

対象製品について、[IX-SOFT]のみ PC アプリケーションですが、インターホン端末と同等のセキュリティ強化方法となる場合がありますのでご注意ください。

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

暗号方式を変更可能な機能は以下の通りです。

通信が暗号化されるようシステム支援ソフトの以下項目より設定を行ってください。

■インターホン端末 (IX-SOFT 含む)

◆SMTP 暗号化方式

以下の製品では SMTP 通信を暗号化するよう設定することができます。

設定の際は「TLS」または「STARTTLS」を設定することを推奨いたします。

◇暗号化方式

- ・なし
- ・TLS
- ・STARTTLS

◇対象製品

「対象製品一覧」参照

◇設定項目

- ・IXG システム: [機能設定] ⇒ [メール設定] ⇒ [SMTP 暗号化]
- ・IX システム: [機能設定] ⇒ [メール設定] ⇒ [SMTP 暗号化]

※詳細な設定方法はシステム支援ソフトの取扱説明書参照(4 章にリンク記載)

■PC アプリケーション(IX-SOFT 以外)

本章は対象外です

■スマートフォンアプリケーション

本章は対象外です

2.2 不要なサービスの無効化

使用していないサービスは直ちにセキュリティ上の脅威となることはありませんが、不必要なリスクを軽減するために、不要なサービスは無効にすることを推奨いたします。

●強化方法

■インターホン端末(IX-SOFT 含む)

利用環境によって不要になる可能性のある機能は以下の通りです。利用しない場合はシステム支援ソフトの以下項目より設定を行ってください。

◆NTP の利用有無

◇設定項目

・IXG システム: [ネットワーク設定] ⇒ [NTP] ⇒ [NTP の利用]

(施工者設定のみ設定可)

・IX システム : [ネットワーク設定] ⇒ [NTP] ⇒ [NTP の利用]

※詳細な設定方法はシステム支援ソフトの取扱説明書参照(4 章にリンク記載)

◇対象製品

[対象製品一覧] 参照

【補足】

2.5「正しい日時に設定」に記載のあるように

可能であれば NTP を用いた時刻同期を行うことが推奨されます。

接続可能な NTP サーバがない場合や、

手動での時刻設定を行っている場合に限り本設定での無効化を行ってください。

◆CGI 機能の利用有無

◇設定項目

- ・IXG システム:[機能設定] ⇒ [CGI] ⇒ [CGI 機能の使用] (施工者設定のみ設定可)
- ・IX システム:[機能設定] ⇒ [CGI] ⇒ [CGI 機能の使用]

※詳細な設定方法はシステム支援ソフトの取扱説明書参照(4 章にリンク記載)

◇対象製品

[対象製品一覧] 参照

◆SIF 機能の利用有無

◇設定項目

- ・IXG システム:[機能設定] ⇒ [SIF] ⇒ [SIF 機能の使用] (施工者設定のみ設定可)
- ・IX システム:[機能設定] ⇒ [SIF] ⇒ [SIF 機能の使用]

※詳細な設定方法はシステム支援ソフトの取扱説明書参照(4 章にリンク記載)

◇対象製品

[対象製品一覧] 参照

CGI、SIF の機能については以下をご覧ください

<https://www.aiphone.co.jp/products/business/bizpark/2023/09/001064.html>

■PC アプリケーション(IX-SOFT 以外)

本章は対象外です

■スマートフォンアプリケーション

本章は対象外です

2.3 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「情報セキュリティ方針」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。

※脆弱性の対策はすべての修正が更新履歴に記載されているわけではありません。

●強化方法

■インターホン端末 (IX-SOFT 含む)

リリースされたソフトウェアおよびファームウェアは以下サイトよりダウンロードすることが可能です。定期的に確認し、最新バージョンがリリースされていれば バージョンアップを行ってください。バージョンアップはシステム支援ソフトの以下メニューから手動で実施することができます。

◇設定項目

・IXG システム: [メンテナンス設定] ⇒ [ファームウェア更新]

・IX システム: [メンテナンス設定] ⇒ [ファームウェア更新]

※詳細な設定方法はシステム支援ソフトの取扱説明書参照 (4 章にリンク記載)

◇対象製品

[対象製品一覧] 参照 (IX-SOFT も対象)

◇ソフトウェア・ファームウェアリリース場所

・IXG システム

<https://www.aiphone.net/support/software-documents/ixg/>

<https://www.aiphone.co.jp/products/business/ixg/product-list/>

・IX システム

<https://www.aiphone.net/support/software-documents/ix/>

<https://www.aiphone.co.jp/products/business/ix/product-list/>

また、IXGW-GW、IXGW-TGW は自動バージョンアップ機能があり、ファームウェアがリリースされた後、特定のタイミングで自動バージョンアップされます。

■PC アプリケーション (IX-SOFT 以外)

PC アプリケーションでは最新バージョンのインストーラから再度インストールを実施することでバージョンアップが可能です。以下にてインストーラを展開していますので、定期的に確認し、最新バージョンがリリースされていれば バージョンアップを行ってください。

◇対象製品

IX-SOFT 以外の PC アプリケーション

◇ソフトウェア・ファームウェアリリース場所

・IXG システム

<https://www.aiphone.co.jp/products/business/ixg/product-list/>

<https://www.aiphone.net/support/software-documents/ixg/>

・IX システム

<https://www.aiphone.co.jp/products/business/ix/product-list/>

<https://www.aiphone.net/support/software-documents/ix/>

■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。

◇対象製品

すべてのスマートフォンアプリケーション

◇ソフトウェア・ファームウェアリリース場所

・IXG インターホンアプリ(iOS 版)

<https://apps.apple.com/jp/app/aiphone-ixg/id1444561862>

・IXG インターホンアプリ(Android 版)

<https://play.google.com/store/apps/details?id=jp.co.aiphone.ixgsystem&pli=1>

2.4 安全なパスワードの設定

パスワードの管理においては、パスワードを攻撃者が推測できない値かつ他のサービスと使いまわさない値を設定することが重要です。

パスワードが意図しない第三者により特定された場合は攻撃者による不正アクセスにつながり、機器情報の漏洩や機器の不正操作などにつながる可能性があります。

パスワードは使いまわしを避けて必ず推測が困難な安全な値となるように設定してください。また意図しない第三者にパスワードが漏洩しないよう、パスワードは適切に管理を行ってください。

パスワードは以下に沿って設定を行えば、安全な値に設定することが可能です。

設定を行う際は以下を参考にパスワードの作成を行ってください。

○安全な ID・パスワードの設定内容

- ① ID とパスワードを同じ文字列にしない
- ② 数字、アルファベット(大文字・小文字)を組み合わせる
- ③ 連続した数字やアルファベットにしない
- ④ 8 文字以上の長さのパスワードに設定する。
- ⑤ デフォルトのパスワードは使用しない
- ⑥ 複数の単語をランダムに組み合わせるパスフレーズの利用により覚えやすく長いパスワードを用いる

●強化方法

■インターホン端末 (IX-SOFT 含む)

インターホン端末ではシステム支援ソフトより「管理者」「一般利用者」「ONVIF」「RTSP」に対してパスワードを設定することができます。各パスワードによって以下の通り、設定値に制限があるため、設定値は以下の通り、制約がございます。以下の制約にも考慮しつつ強固なパスワードの設定を行ってください。

◇設定項目

・IXG システム:[端末設定] ⇒ [パスワード]

・IX システム:[基本情報登録] ⇒ [パスワード]

※詳細な設定方法はシステム支援ソフトの取扱説明書参照(4 章にリンク記載)

◇制約事項

・管理者パスワード

半角英数 1-32 文字 ※「admin」は設定できません

・「一般利用者」「ONVIF」「RTSP」のパスワード

半角英数 1-32 文字

◇対象製品

パスワードが設定可能な製品は設定するアカウントごとに異なります。

【管理者】

[対象製品一覧] 参照 (IX-SOFT も対象)

【一般利用者】

[対象製品一覧] 参照 (IX-SOFT も対象)

【ONVIF】

[対象製品一覧] 参照

【RTSP】

[対象製品一覧] 参照 (IX-SOFT も対象)

■PC アプリケーション (IX-SOFT 以外)

IX・IXG のシステム支援ソフト・監視ソフトではログインするための管理者 ID・管理者パスワードを設定することができます。また、IXG のシステム支援ソフトでは最大 10 件の施工者・管理者のアカウントにパスワードを設定することができます。

設定値は以下の通り、制約がございます。以下の制約に考慮しつつ強固なパスワードの設定を行ってください。

◇設定項目

- ・IXG システム: [ファイル(F)] ⇒ [環境設定] ⇒ [ID、パスワード設定]
 - ・IX システム: [編集(E)] ⇒ [システム支援ソフトの設定] ⇒ [ID、パスワード設定]
 - ・IXG システム(アカウント): [ファイル] ⇒ [システム支援ソフトアカウント管理]
- ※詳細な設定方法はシステム支援ソフトの取扱説明書参照 (4 章にリンク記載)

◇ID・パスワード 制約事項

- ・半角英数 1-32 文字
- ・「admin」は再設定できません。※デフォルト値は ID・パスワードともに「admin」です。

◇対象製品

IX-SOFT 以外の PC アプリケーション

【補足】

IXG システム支援ソフトでは初めてログインする場合にパスワード変更画面が表示されます。この画面より必ずデフォルトパスワードからのパスワード変更を行ってください。

■スマートフォンアプリケーション

本章は対象外です

2.5 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や有効期限切れの証明書による不正アクセスなど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。

日時の設定は NTP サーバと同期させておくことを推奨しています。信頼できる NTP サーバと同期することで設定される日時情報の精度を高め、日時情報のずれも自動で修正することができます。また、NTP サーバの利用が難しい場合も手動での日時設定が可能ですので正しい日時に設定をおこなってください。

●強化方法

■インターホン端末

インターホン端末では NTP サーバとの同期設定、手動での日時設定をシステム支援ソフト・WEB 設定にて実施できます。(WEB 設定は IX システムのインターホン端末でのみ実施可能)それぞれの設定はシステム支援ソフト・WEB 設定の以下のメニューから実施することが可能です。詳細はシステム支援ソフトの取扱説明書をご確認ください。(4 章にリンク記載)

◇NTP 設定

- ・IXG システム: [ネットワーク設定] ⇒ [NTP]
(施工者設定のみ設定可)
- ・IX システム: [ネットワーク設定] ⇒ [NTP]
(メニューはシステム支援ソフト・WEB 設定で同様)

◇手動での日時設定

- ・IXG システム: [端末設定] ⇒ [時刻合わせ]
 - ・IX システム: [基本情報登録] ⇒ [時刻合わせ]
(メニューはシステム支援ソフト・WEB 設定で同様)
- ※詳細な設定方法はシステム支援ソフトの取扱説明書参照(4 章にリンク記載)

◇対象製品

対象製品は[NTP 設定] [手動での日時設定]ごとに異なります。
詳細は[対象製品一覧]をご確認ください。

【補足】

IXG システムでは、IXGW-GW ゲートウェイアダプターのあるシステムの場合、デフォルトで NTP が有効になり、アイホン NTP サーバアドレス（ntp.jo.aiphone-app.net）が設定されます。

IX システムにおいてもアイホン NTP サーバアドレス（ntp.jo.aiphone-app.net）が利用可能ですので本アドレスを指定されることを推奨します。

また LAN 内に NTP サーバがある場合は代わりにそのサーバを利用されることを推奨します。

■PC アプリケーション

PC アプリケーションの時刻はインストールしている PC や OS の時刻設定に紐づきます。

ご使用の PC や OS の設定手順に沿って、NTP サーバとの同期設定・手動での日時設定を行ってください。

◇対象製品

すべての PC アプリケーション

■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時刻はインストールしているスマートフォンや OS の時刻設定に紐づきます。ご使用のスマートフォンや OS の設定手順に沿って、時刻同期・手動での日時設定を行ってください。

◇対象製品

すべてのスマートフォンアプリケーション

【補足】

スマートフォンが携帯回線（Mobile Network）と接続されている状態であれば、回線からの情報を基に自動的に時刻同期がされます。（明示的に手動で日時を設定している場合を除きます）

2.6 権限の分離

IXG、IX システムでは製品毎にいくつかの権限があり、各権限でしか実施できない機能が存在します。各権限には ID、パスワードが設定されますが、それらが分かれば不正に機能を利用することができるため、各権限の ID、パスワードは適切な利用者にのみ伝えるようにしてください。

また、ID、パスワードの取り扱いにも注意が必要です。作成された各権限の ID、パスワードは悪意あるものに窃取されないよう管理してください。

●強化方法

■インターホン端末(IX-SOFT 含む)

インターホン端末には管理者権限・一般利用者権限の2種類の権限が存在し、システム支援ソフト・WEB 設定より設定することができます。これらの権限ではそれぞれ以下の機能を使用することが可能です。以下の機能に沿って適切な利用者により各権限の ID、パスワードを伝えるようにしてください。

【補足】

WEB 設定は IX システムのインターホン端末のみ実施可能です。

◇対象機能

1.管理者権限

- ・システム支援から端末へ設定変更
- ・CGI 機能
- ・端末の画面から設定モードへのログイン (IX-MV7、IX-SOFT のみ)

2.一般利用者権限

- ・CGI 機能

◇対象製品

[対象製品一覧] 参照 (IX-SOFT も対象)

■PC アプリケーション (IX-SOFT を除く)

PC アプリケーションには利用するための権限が存在し、ID・パスワードが付与されます。

そのため、各 PC アプリケーションの適切な利用者により ID・パスワードを伝えるようにしてください。また、IXG システム支援ソフトの場合は管理者権限・施工者権限の2種類の権限が存在します。以下に沿って適切な利用者により各権限の ID、パスワードを伝えるようにしてください。

◇対象権限

1.施工モード権限

IXG システム支援ソフトのすべての設定項目が設定可能

2.管理モード権限

以下の項目のみ設定可能

- ・入居設定

- ・退去設定
- ・詳細設定

◇対象製品

IX-SOFT 以外の PC アプリケーション

■スマートフォンアプリケーション

本章は対象外です。

2.7 権限の適切な失効

IXG、IX システムでは製品毎にいくつかの権限があり、各権限でしか実施できない機能が存在します。各権限には ID、パスワードが設定されますが、それらが分かれば不正に機能を利用することができます。担当者が変更になった場合や利用グループが変化した場合などに昔の担当者の権限を確実に落とすためにアカウントの失効および管理者パスワードの変更を行うようにしてください。

●強化方法

■インターホン端末(IX-SOFT 含む)

インターホン端末には管理者権限・一般利用者権限の2種類の権限が存在し、システム支援ソフト・WEB 設定より設定することができます。これらの権限ではそれぞれ以下の機能を使用することが可能です。管理者や一般利用者の変更があった際は適切にアカウントの失効もしくはパスワードの変更を行うようにしてください。

【補足】

WEB 設定は IX システムのインターホン端末のみ実施可能です。

◇設定項目

- ・IXG システム:[端末設定] ⇒ [パスワード]
- ・IX システム:[基本情報登録] ⇒ [パスワード]

※詳細な設定方法はシステム支援ソフトの取扱説明書参照(4 章にリンク記載)

◇対象機能

1.管理者権限

- ・システム支援から端末へ設定変更
- ・CGI 機能
- ・端末の画面から設定モードへのログイン(IX-MV7、IX-SOFT のみ)

2. 一般利用者権限

- ・ CGI 機能

◇ 対象製品

[対象製品一覧] 参照 (IX-SOFT も対象)

■ PC アプリケーション (IX-SOFT を除く)

PC アプリケーションには利用するための権限が存在し、ID・パスワードが付与されます。

そのため、各 PC アプリケーションの適切な利用者によりのみ ID・パスワードを設定するようにしてください。

また、IXG システム支援ソフトの場合は管理者権限・施工者権限の2種類の権限が存在します。管理者や一般利用者の変更があった際は適切にアカウントの失効もしくはパスワードの変更を行うようにしてください。

◆ ID、パスワード

◇ 設定項目

- ・ IXG システム: [ファイル(F)] ⇒ [環境設定] ⇒ [ID、パスワード設定]
 - ・ IX システム: [編集(E)] ⇒ [システム支援ソフトの設定] ⇒ [ID、パスワード設定]
- ※ 詳細な設定方法はシステム支援ソフトの取扱説明書参照 (4 章にリンク記載)

◇ 対象権限

1. 施工モード権限

IXG システム支援ソフトのすべての設定項目が設定可能

2. 管理モード権限

以下の項目のみ設定可能

- ・ 入居設定
- ・ 退去設定
- ・ 詳細設定

◇ 対象製品

IX-SOFT 以外の PC アプリケーション

◆ システム支援ソフトアカウント管理 (施工者権限でのみ設定可)

◇ 設定項目

・IXG システム:[ファイル] ⇒ [システム支援ソフトアカウント管理]

※詳細な設定方法はシステム支援ソフトの取扱説明書参照(4 章にリンク記載)

◇対象製品

IXG システム支援ソフト

■スマートフォンアプリケーション

本章は対象外です。

2.8 TLS 証明書(SSL 証明書)に対するセキュリティ強化

IX・IXG システムのインターホン端末では TLS 証明書(SSL 証明書)を導入することで以下のセキュリティ強化を行っています。

- ・WEB 設定やインターホン端末間の TLS 通信
- ・インターホン端末間のなりすまし防止
- ・WEB 設定で表示される警告文による中間者攻撃等の保護

しかし、証明書の有効期限が切れると上記のセキュリティ強化が適切に行われない可能性があります。IXG、IX システムではシステム支援ソフトを使用することでインターホン端末に導入された証明書を更新することが可能です。導入された証明書を適切に管理し、有効期限が切れる前に更新を行ってください。

●強化方法

■インターホン端末

インターホン端末の証明書を更新するためには、ご自身で証明書を作成する必要があります。システム支援ソフトでは証明書発行に必要な署名リクエスト(CSR)を作成することが可能です。以下の流れで 1.署名リクエスト～3.証明書更新まで実施してください。

◇証明書更新手順

1. 署名リクエスト(CSR)作成

署名リクエスト(CSR)の作成をおこないます。システム支援ソフトから以下を開き、必須事項を入力して作成してください。

(作成した CSR には RSA-2048 の鍵ペアが内部で生成されます)

[機能設定] ⇒ [署名リクエスト生成] (施工者設定のみ設定可)

2. 証明書発行

作成した署名リクエストを使用し認証局へサーバ証明書の発行を依頼します。

依頼方法は各認証局で明示された手順で実施してください。

3. 証明書設定アップロードする証明書をシステム支援ソフトに設定します。システム支援ソフトから以下を開き、[2 で発行したサーバ証明書]、必要に応じて[2 で発行を依頼した認証局の CA 証明書]を設定してください。

[機能設定] ⇒ [SSL 証明書]（施工者設定のみ設定可）

4. 証明書アップロード

システム支援ソフトから以下を開き、3 で設定した証明書をインターホン端末にアップロードします。

[機能設定] ⇒ [SSL 証明書] ⇒ [SSL 証明書のアップロード]

（施工者設定のみ設定可）

【補足】

インターホン端末には PEM 形式の証明書のみアップロード可能です。証明書を発行する際は PEM 形式のサーバ証明書を発行してください。

※詳細な実施方法はシステム支援ソフトの取扱説明書をご確認下さい

（4 章にリンク記載）

○対象: インターホン端末

[対象製品一覧]参照

■PC アプリケーション (IX-SOFT を除く)

本章は対象外です。

■スマートフォンアプリケーション

本章は対象外です。

2.9 IEEE802.1X 認証方式のセキュリティ強化

IX・IXG システムのインターホン端末では IEEE802.1X 認証方式を導入することで以下のセキュリティ強化を行っています

・インターホン端末と RADIUS サーバの相互認証

しかし、IEEE802.1X 認証方式で使用する証明書は定期的に更新を行わないと上記のセキュリティ強化が適切に行われない可能性があります。IXG、IX システムではシステム支援ソフトを使用することでインターホン端末に導入された証明書を更新することが可能です。導入された証明書を適

切に管理し、以下の手順で更新を行ってください。

●強化方法

■インターホン端末

インターホン端末の証明書を更新するためには、ご自身で証明書を作成する必要があります。システム支援ソフトでは証明書発行に必要な署名リクエスト(CSR)を作成することが可能です。以下の流れで 1.署名リクエスト～4.証明書更新まで実施してください。

◇証明書更新手順

1. 署名リクエスト(CSR)作成

クライアント証明書の発行には署名リクエスト(CSR)が必要です。IEEE802.1X 認証方式の場合、システム支援ソフトでは CSR を作成することができません。そのため、ご自身で CSR の作成を行ってください。また、CSR 作成時の必要な鍵ペアの暗号方式・鍵長はそれぞれ以下であれば対応可能です。

- ・暗号方式: AES-256
- ・鍵長: 256 ビット

2. 証明書発行

作成した署名リクエストを使用し認証局へクライアント証明書の発行を依頼します。依頼方法は各認証局で明示された手順に従って実施してください。

3. IEEE802.1X 認証設定

インターホン端末より IEEE802.1X 認証を行う場合は設定が必要です。
システム支援ソフトから以下を開き、設定を行ってください。

[機能設定] ⇒ [IEEE 802.1X] (施工者設定のみ設定可)

また、EAP 方式によって設定方法が異なります。以下を参考に設定を行ってください。

・PEAP の場合

EAP 方式: 「PEAP」に設定
EAP ユーザー名: 設定必要
EAP パスワード:

・TLS の場合

EAP 方式: 「TLS」に設定
EAP ユーザー名: 設定必要
EAP パスワード: 設定不要

4. 証明書アップロード

発行したクライアント証明書をインターホン端末へアップロードします。システム支援ソフトから以下を開き、証明書・秘密鍵を設定後、インターホン端末へアップロードをします。

[機能設定] ⇒ [IEEE 802.1X] (施工者設定のみ設定可)

また、EAP 方式によってアップロードが必要なファイルが異なります。以下を参考に設定を行ってください。

・PEAP の場合

CA 認証ファイル: 必要 (2 で発行を依頼した CA の CA 証明書を設定)

クライアント認証ファイル: 不要

秘密鍵(クライアントプライベートキー): 不要

・TLS の場合

CA 認証ファイル: 必要 (2 で発行を依頼した CA の CA 証明書を設定)

クライアント認証ファイル: 必要 (2 で発行したクライアント証明書を設定)

秘密鍵(クライアントプライベートキー): 必要 (1 で使用した鍵ペアの秘密鍵を設定)

【補足】

インターホン端末には PEM 形式の証明書のみアップロード可能です。証明書を発行する際は PEM 形式のサーバ証明書を発行してください。

※ 詳細な操作方法是システム支援ソフトの取扱説明書をご確認下さい。(4 章にリンク記載)

○対象: インターホン端末

[対象製品一覧]参照

■PC アプリケーション (IX-SOFT を除く)

本章は対象外です。

■スマートフォンアプリケーション

本章は対象外です。

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

IX・IXG システムで使用されるインターホン端末・PC・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

インターホン端末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。

◇セキュリティワイヤーの取り付け

据え置き型のインターホン端末や PC には可能であればセキュリティワイヤー等を取り付け、盗難できないようにしてください。

◇画面ロックの設定

使用する PC やスマートフォンはパスワードの入力を強要するよう、画面ロックの設定を行い、盗難されたとしても使用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。

◇監視ソフトによるインターホン端末の監視

監視ソフトを導入すれば、同ネットワークに接続されているインターホン端末の監視を行うことができます。IX/IXG 監視ソフトより定期的に監視を行い、異常を検知した際にポップアップの表示・メールの送信がされることでインターホン端末が盗難された場合でも管理者へ通知され早急に対応を行うことができます。可能な限り、監視ソフトを導入し、インターホン端末の監視を行うようにしてください。

※監視ソフトの詳細な利用方法は取扱説明書をご確認ください。(4 章にリンク記載)

3.2 システムを構築するネットワーク製品(スイッチングハブ・ルータ) への対策

IX・IXG 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(スイッチングハブ・ルータ)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 IX・IXG 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 IX・IXG 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。使用する LAN ケーブルについても露出しないよう施工することを推奨いたします。

また、ルータの場合は無線機能を使用しない場合は Wi-Fi を OFF にすることも有効です。

◇定期的なファームウェア更新

使用しているネットワーク製品について、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(ルータの場合は SSID やパスワード)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(ルータの場合のみ)

IXG インターホンアプリがインストールされたスマートフォンをルータ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(WPA3 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(ルータの場合のみ)

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、不要な場合は無効に設定することを推奨いたします。

3.3 使用する PC・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 PC、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セキュリティ強度も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マルウェアに対する定義ファイルが含まれており、セキュリティ強度を向上させることができます。また、当社 PC アプリケーション・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。

IX・IXG 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 IX・IXG システムのセキュリティ強化が見込めます。

○IX・IXG 使用ポート一覧

付表 2_使用ポート一覧_(IX システム・IXG システム).pdf

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

取扱説明書のリンクは以下を参照ください。

○IX システム支援ソフト 取扱説明書

英語: <https://www.aiphone.net/support/software-documents/ix/documents.html>

日本語: https://www.aiphone.co.jp/data/product_data/item_search_detail.php?prod_no=IX-MV7-HB

○IXG システム支援ソフト 取扱説明書

英語: <https://www.aiphone.net/support/software-documents/ixg/documents.html>

日本語: https://www.aiphone.co.jp/data/product_data/item_search_detail.php?prod_no=IX-MV7-HB

○IX 監視ソフト 取扱説明書

英語: <https://www.aiphone.net/support/software-documents/ixg/documents.html>

日本語: https://www.aiphone.co.jp/data/product_data/item_search_detail.php?prod_no=IX-MV7-HB

○IXG 監視ソフト 取扱説明書

英語: <https://www.aiphone.net/support/software-documents/ix/documents.html>

日本語: https://www.aiphone.co.jp/data/product_data/item_search_detail.php?prod_no=IX-MV7-HB

- ・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。
- ・Microsoft、Windows は、米国 Microsoft Corporation 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。