そのカメラ、 正しく設定できていますか？

インターネットに接続されたカメラは第三者が簡単に見つけることができます

インターネットからアクセス可能なカメラは、検索サイトを使って探し出すことが可能です。その検索結果から脆弱性のあるカメラを自動で洗い出すツールも確認されています。
必要で無い限り IP カメラをインターネットに接続しないようにしましょう。

IP カメラへの不正アクセスがニュースになりました

【原因は初期パスワードのまま利用していたこと】
IP カメラの操作には、通常パスワードが要求されます。このパスワードが初期値のままになっていると、製品マニュアルの情報を参照できるすべての人がIPカメラを不正に操作できます。

また、IP カメラの普段使わないサーバ機能を動作させていると、それらを悪用されてマルウェアに感染することがあります。マニュアルを見て不要なサーバ機能は停止しましょう。

更に、IP カメラには利用者が停止できないバックドアと言われる侵入口が存在する場合があります。バックドアが発見されると、それを塞いだ新しいバージョンのファームウェアが製品のサイトに公開されます。設置する IP カメラが最新のファームウェアかどうかを確認しましょう。

IP カメラ安全利用のためのチェックリスト

- ☐ むやみに IP カメラをインターネットに接続しない
- ☐ IP カメラにログインできるパスワードは初期値から変更する
- ☐ Web 以外の不要なサーバ機能は停止する
- ☐ IP カメラの製品サイトを確認し、バージョンアップする

IP カメラを導入するときは、これ以外にも接続元の制限や正しく動いていることの確認など、設置や運用において気を付けなければいけないことがあります。

詳しくは、IPA で公開している、
「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」
を参照してください。

https://www.ipa.go.jp/security/jisec/choutatsu/nwcs/checklist_nwc.pdf

IPA 独立行政法人情報処理推進機構
特定用途機器情報セキュリティ対策検討委員会

JISEC-PROC-2018-A03