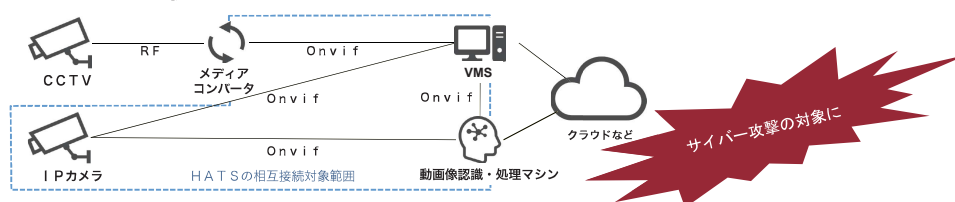


IP カメラのセキュリティの確保に向けた取り組み

IPカメラのセキュリティ事故の事例を分析し
対策ガイドラインの広報活動を行っています

高度化するカメラ

従来監視カメラはクローズドな環境で運用されていましたが、AI などの恩恵を受けるために常時ネットワークに接続できる状態にしておくケースが増えています。



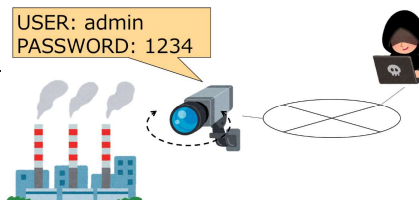
IP カメラシステムも PC などと同等の対策が必要です！

事例 1: パスワード推測による不正アクセス

機器を守る
ポイント1

必ず初期設定以外の類推が困難なパスワードの設定を徹底しましょう

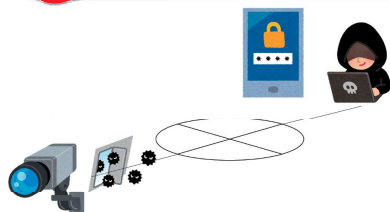
初期設定されたユーザ名やパスワードは、メーカー毎にほぼ決まっていたり、Web サイトなどから入手可能な説明書に掲載されているため、誰でも知ることができます。



事例 2: 脆弱性によるパスワードなどの漏洩

機器を守る
ポイント2

メーカーの Web ページや脆弱性情報データベース (JVN) などをこまめに確認しファームウェアを更新しましょう



パスワードなどが暗号化されずに送信などの脆弱性をもつファームウェアが適用されていた場合、悪意のある第三者は、それらの脆弱性を悪用して、不正にアクセスされるだけではなく、ユーザ名やパスワードそのものを入手することが可能な場合があります。

事例 3: 不正アクセスによる機器の“踏み台”化

機器を守る
ポイント3

必要に応じてカメラを外部ネットワークから分離するかファイアウォールなどを設置しましょう

第三者が機器のファームウェアを比較的容易に書き換えることができます。ファームウェアを書き換えることにより、他のシステムに対する DDoS 攻撃などの踏み台にされてしまうなど、第三者への攻撃に意図せず加担してしまうことがあります。