CIAJ セキュリティ Information

監視カメラシステムセキュリティの基礎
～脅威と対策～

2018 年 7 月 25 日

CIAJ 通信ネットワーク機器セキュリティ分科会

はじめに

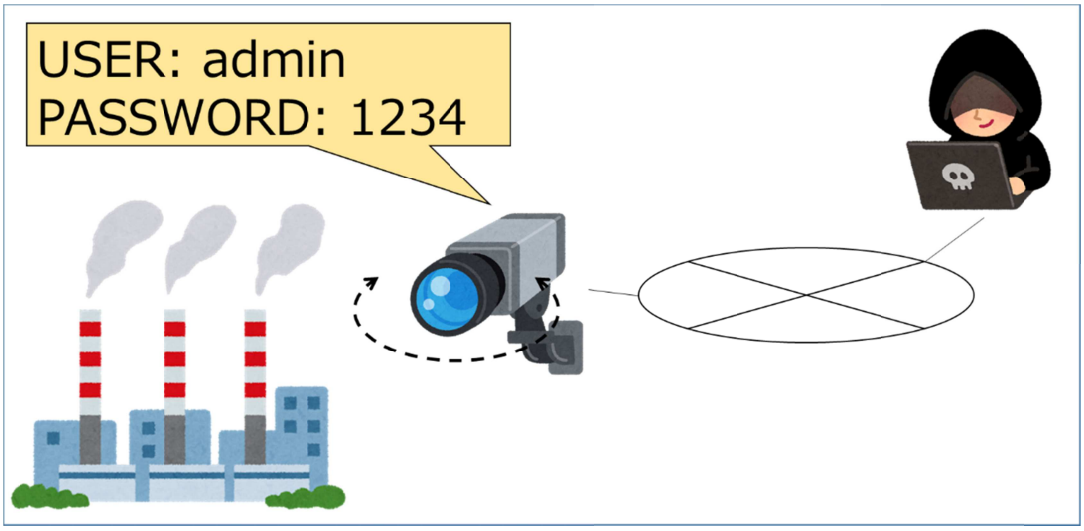
「IoT」という言葉が一般に用いられるようになる中、インターネットに接続される機器が普及するとともに、そのセキュリティに対する関心も高まっています。

監視カメラシステムにおいても、一般向けや業務向けの製品問わず、監視カメラやレコーダ装置、管理装置などをインターネットに接続するケースが増加しており、設置者が意図しない第三者による映像閲覧等、各種のセキュリティに対する脅威の事例が TV ニュースなどで取り上げられるなど、社会的な関心を集めています。

本記事では、監視カメラシステムを利用する際に問題となりやすい代表的な脅威の事例とその対策を紹介します。

事例紹介　～脅威と対策

（事例１）初期パスワードや脆弱なパスワードの利用に起因する、第三者による映像不正閲覧・PTZ 等の機器操作

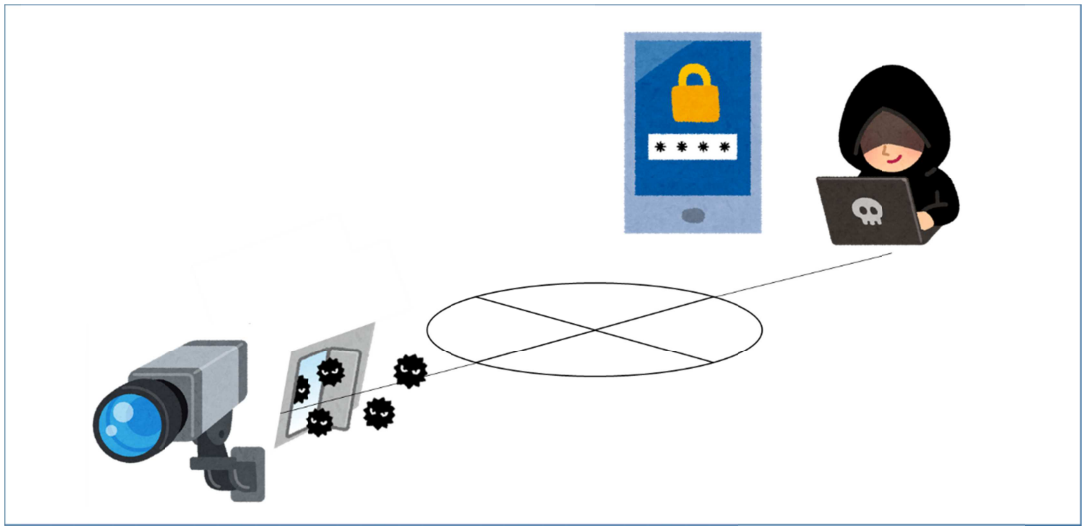


【脅威】監視カメラなどに初期設定されたユーザ名やパスワードは、メーカ毎にほぼ決まっていたり、WEB サイトなどから入手可能な説明書に掲載されているなど、誰でも知ることができると考えるべきでしょう。また、類推容易であるなど、脆弱なユーザ ID やパスワードを用いている場合、人手、あるいはプログラムによる総当り攻撃(ブルートフォースアタック)などで把握されてしまう可能性があります。監視カメラなどのユーザ名とパスワードが第三者に把握されてしまった場合、意図しない監視映像の閲覧が行われたり、各種設定、PTZ を含む様々な制御が行われてしまう危険性があります。また、このように閲覧可能な監視カメラをまとめてインデックス化し、全世界に公開しているサーバがあることが知られています。

【対策】導入する機器には、パスワードの類推が困難となるように、パスワードに含まれる文字の種類や文字数に制約が設けられていたり、一定回数のパスワード試行失敗時に、一定時間ログイン不可となるような機能が実装されていることが望ましいです。

また、運用時には、初期パスワードの変更を必須とし、IPA ガイドラインなどに基づき類推困難なパスワードに設定することが望まれます。また、機器に対し意図しないアクセスが行なわれることの無いよう、必要が無ければ外部ネットワークと分離したり、IP アドレスやホスト名などに基づきネットワークアクセスを制限することが必要です。

（事例２）脆弱性のあるファームウェアによるユーザ ID・パスワード漏えい

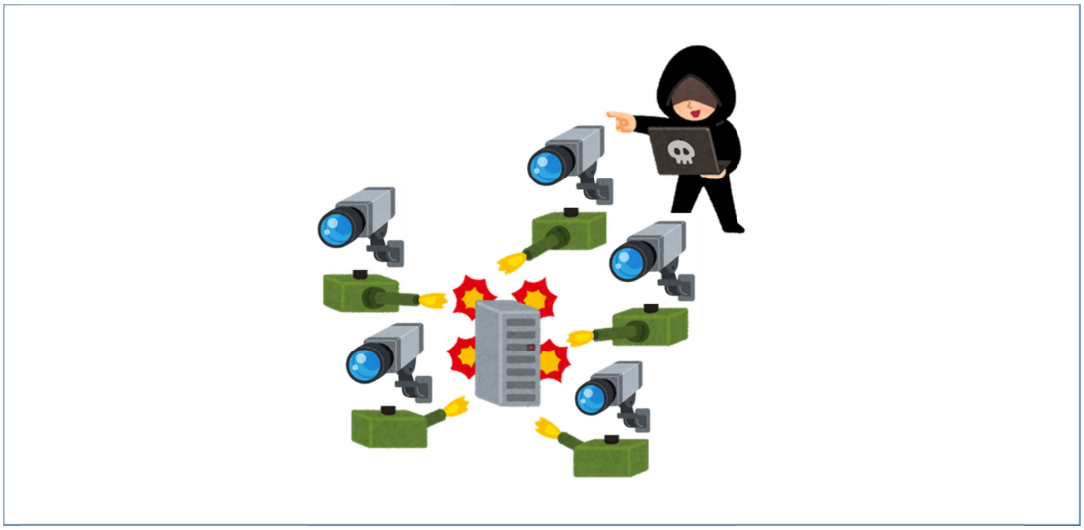


【脅威】ユーザ ID やパスワード、あるいは、それらを類推可能な情報がネットワーク上に流れたり、URI などに含まれてしまうなどの脆弱性をもつファームウェアが監視カメラなどの機器に適用されていた場合、悪意のある第三者は、それらの脆弱性を利用して、ユーザ名やパスワードを入手することが可能です。入手したユーザ名やパスワードを用いることによって、対象となる監視カメラなどの機器は、事例１に示したように思いのままに利用することが可能になります。

【対策】販売元のサイトなどで脆弱性情報の公開や、ファームウェアの更新版の提供が継続的になされているかなど、サポート体制が整備されているか、また、信用に足る実績があるかなど、機器選定の際に事前に確認を行いましょう。また、手順が分かりやすく、簡単にファームウェア更新ができる機能を備える機器を導入しましょう。

導入の際、一般に公開されているツール等を活用して脆弱性の有無を確認し、可能であればその脆弱性への対策をとることが望ましいです。また、導入時には、その時点で公開されている最新のファームウェアに更新すると共に、新しいファームウェアが公開された場合には、速やかにファームウェアアップデートを実施することが求められます。

（事例３）不正なファームウェア適用による「踏み台」化



【脅威】事例１や事例２に示したような手段でユーザ ID とパスワードを入手することにより、悪意のある第三者が管理者権限を取得し、監視カメラなどの機器に備わっているファームウェアの更新機能を利用したり、ファームウェアの脆弱性を利用することによって、対象となる機器に不正なファームウェアを適用し、他のシステムに対する DDoS 攻撃の踏み台として利用するなど、第三者への攻撃に意図せず加担してしまいます。

【対策】システム構築時には、機器の脆弱性を突かれる機会が少なくなるように、必要が無ければ外部ネットワークから分離する、また、外部ネットワークとの接続が必要であれば、ルータやファイアウォールを設置したり、機器側で IP アドレス等によりネットワークアクセスを限定することが望まれます。また、機器側は、不要なサービスは停止するようにしましょう。

ネットワーク経由でファームウェアアップデートに対応している機器の場合、ファームウェア配信サーバとの通信路が暗号化されることを確認するとともに、機器側はサーバ証明書を検証する、また、アップデートファイルの電子署名を検証する機能を備えた機器を導入しましょう。また、ファームウェアの改ざん検知機能を備え、改ざんされた場合に備えて、工場出荷状態などに初期化、または、ロールバックすることができる機能を備えていることが求められます。

また、ネットワーク経由でのファームウェアアップデートに対応していない機器の場合は、正式なページからファームウェアを入手し、機器に適用するようにしましょう。

また、万一、踏み台になってしまった場合、あるいは疑わしい場合は、ネットワークから切断し対策を行うことが必要です。

まとめ

本記事では、監視カメラシステムのセキュリティに関し、世間の関心が高い代表的な事例を紹介し、その脅威と対策について説明しました。なお、監視カメラシステムに関わるセキュリティについては、業界団体や公的機関の取り組みにより、より網羅的なセキュリティに関する分析として、システム調達の観点から監視カメラシステムに求められるセキュリティ対策とその要件について述べた「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」(IPA)、公衆インターネット網と接続することを前提にしたネットワーク構成モデルとネットワーク設計について述べた「防犯カメラシステムネットワーク構築ガイドⅡ」(日本防犯設備協会)などが公開されており、システム発注や設計・構築に関わる方は併せて参照していただくようお願いします。

また、開発ベンダや CIAJ を含む業界団体から適宜セキュリティ情報が提供されており、これらの情報を定期的に確認することをお勧めします。

著者

CIAJ マルチメディア通信委員会　IP カメラ接続 WG

参考文献

[1] 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」, 独立行政法人 情報処理推進機構, 2017 年 12 月

[2], 防犯カメラシステムネットワーク構築ガイドⅡ, 公益社団法人 日本防犯設備協会, available at http://www.ssaj.or.jp/guidebook/pdf/421.pdf, 2017 年 4 月