2023年1月30日
株式会社日立産業制御ソリューションズ

弊社ネットワークカメラ・デジタルレコーダー

不正アクセス防止対策に関するご案内

目次

はじめに

ネットワークに接続する機器に対し、意図しない第三者からの不正アクセスによるサイバー攻撃の標的となるケースが増えております。ネットワークカメラにおいても同様でセキュリティ対策をせずに運用すると第三者からの攻撃対象となる危険性が高くなってしまいます。
このような危険性を排除するために、セキュリティポリシーに基づいた対策を講じることで第三者からの攻撃リスクを減らすことができます。

本書では、2020 年 3 月に生産を終了しました弊社ネットワークカメラ、デジタルレコーダーを用いたシステム運用におけるネットワークセキュリティの対応策をご説明いたします。
現在、システム運用されていることとは思いますが、今一度、ご確認いただければ幸いです。

対象機種

■ネットワークカメラ

DI-Cx1xxシリーズ：DI-CB100、DI-CB110、DI-CD100、DI-CD110
DI-Cx2xx シリーズ：DI-CS211、DI-CB200、DI-CD200、DI-CB201、DI-CD201, DI-CB210、DI-CD210、DI-CB211、DI-CD211、DI-CZ211
DI-Cx3xx シリーズ：DI-CB320、DI-CB320G、DI-CB320YT、DI-CD320、DI-CD320G、DI-CD320YT、DI-CF310、DI-CB325、DI-CD325、DI-CD322LE、DI-CD322LEG、DI-CB322LEW、DI-AT325
DI-Cx5xx シリーズ：DI-CB520、DI-CD520、DI-CS520、DI-CF590、DI-CF590i
EZ シリーズ　　：EZ-CB120、EZ-CB120LE、EZ-CD120、EZ-CD120LE、EZ-MD110
HB シリーズ　　：HB-B120LE、HB-D120LE、HB-E110
HC シリーズ　　：HC-IP3000

■デジタルレコーダー

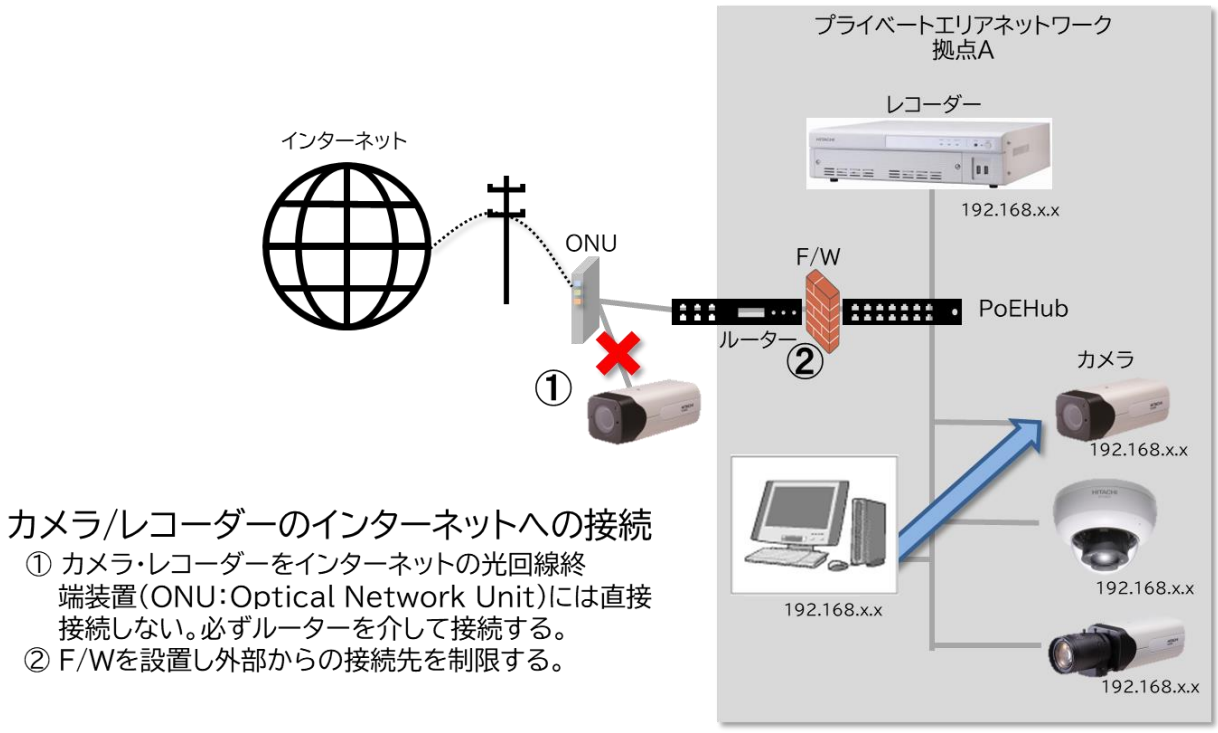
DS-Gxxx シリーズ　：DS-G150、DS-G150H、DS-G230、DS-G250、DS-G260、DS-G260H、DS-G350、DS-G350R、DS-G360、DS-G360H
DS-JHxxx シリーズ　：DS-JH260、DS-JH260YT、DS-JH560、DS-JH580、DS-JH270、DS-JH570、DS-JH590、DS-JH260H、DS-JH560H、DS-JH570H
DS-NRx08シリーズ　：DS-NR108、DS-NR208
DS-NRx000 シリーズ：DS-NR1000、DS-NR2000、DS-NR3000、DS-NR4000

【重要】
ネットワークのセキュリティ対策においては、お客さまにて実施ください。
不正アクセスなどセキュリティ上の問題により発生した直接、間接の損害につきましては、弊社は一切の責任を負いかねます。ご理解のほどよろしくお願いいたします。

1. ネットワークカメラ・デジタルレコーダーを用いたシステム構成について

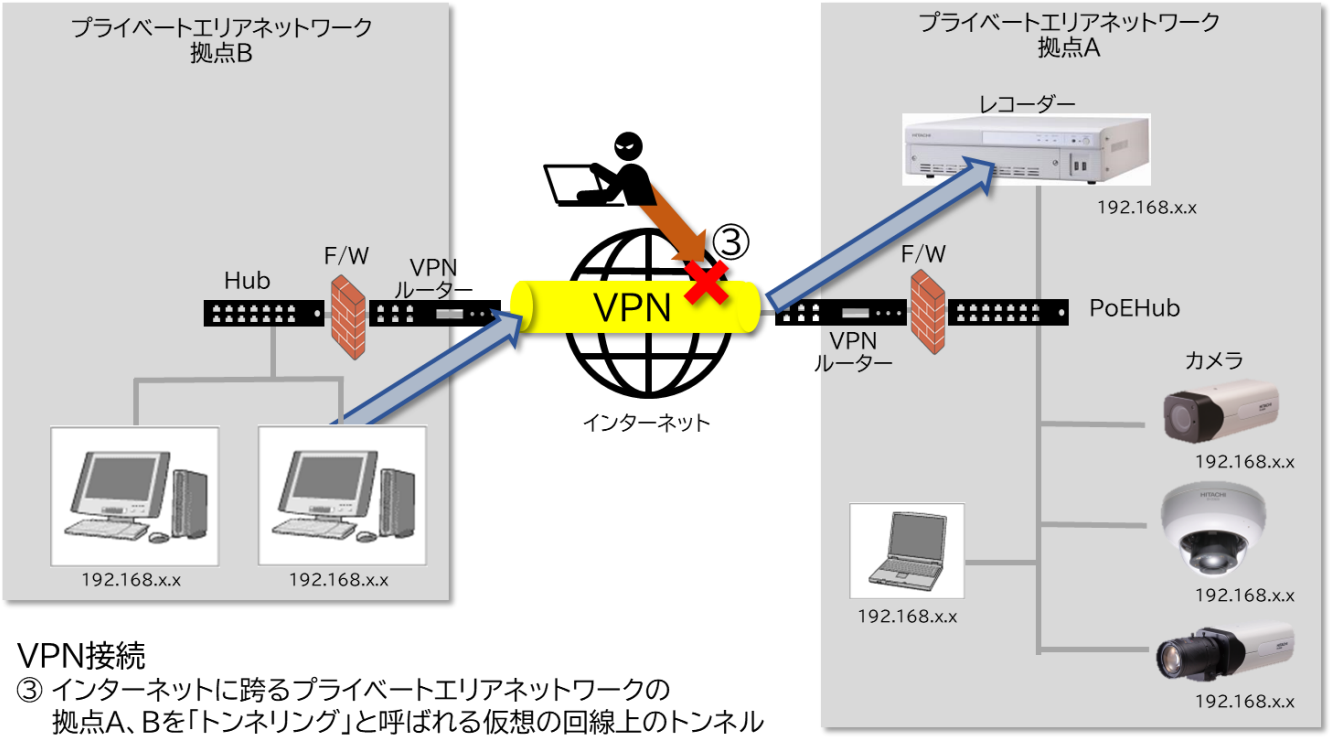
昨今、サイバー攻撃によるシステム停止や情報漏洩のニュースが後を絶ちません。
弊社、ネットワークカメラ・デジタルレコーダーをサイバー攻撃から安心、安全、にご使用いただくためにも、次のようなことにご留意ください。
弊社のネットワークカメラ・デジタルレコーダーは、2020 年 3 月をもって製造を終了しておりますが、現在、運用中のお客さまにおかれましても、再チェックいただき、意図しない第三者からの不正アクセスによるサイバー攻撃に対する備えをご検討ください。

① インターネット回線に直接接続せず、ルーターやファイアウォール(F/W)製品を介して接続してください。
弊社の製品は電気通信事業者(移動通信会社、固定通信会社、インターネットプロバイダなど)の通信回線(公衆無線 LAN を含む)(以下インターネット)に直接接続することができません。本製品をインターネットに接続する場合は、必ずルーターやファイアウォール(F/W)製品などで構築した安全なプライベートネットワークからインターネットにアクセスできる環境で、プライベート IP アドレスを設定して、接続してください。



カメラ/レコーダーのインターネットへの接続
① カメラ・レコーダーをインターネットの光回線終端装置(ONU:Optical Network Unit)には直接接続しない。必ずルーターを介して接続する。
② F/Wを設置し外部からの接続先を制限する。

② インターネットを介して使用する場合は、VPN(Virtual Private Network)接続を推奨します。
インターネットを介するデータの送受信に関しては、VPN 接続を利用するとより安全なセキュリティ環境を構築することができます。VPN 接続のためには、VPN 接続機能を備えたルーターの導入をご検討ください。



VPN接続
③ インターネットに跨るプライベートエリアネットワークの拠点A、Bを「トンネリング」と呼ばれる仮想の回線上のトンネルを設けることで外部からのアクセスを遮断する。

VPN とは？

VPN とは、「Virtual Private Network」の略で、「仮想専用回線」という意味です。「仮想専用回線」とは、あるネットワークの中に、別の仮想的なプライベートネットワーク(ローカルエリアネットワークとも呼ばれる)を作ることをいい、一般的なインターネット回線を利用して接続します。
接続したい拠点(たとえば本社・オフィスなど)に専用のルーターを設置し、公衆の回線を利用して、拠点にある専用ルーターと相互に通信を行います。このとき、公衆の回線上に「トンネリング」と呼ばれる仮想のトンネルを設けることで、拠点間のプライベートネットワークを VPN 接続することで外部ネットワークからのアクセスを遮断することができます。

2. 基本的なセキュリティ対策

不正アクセスによるサイバー攻撃のリスクからネットワークカメラシステムを守るためには、システム全体でのセキュリティ対策の強化することは、前述のとおりではありますが、個々の機器としても、基本的なセキュリティ対策の対応をお願いいたします。

a）弊社の機器納入時の初期のログイン ID やパスワード（以下 PW）は必ず変更してください。
b）PW は、予測しにくい値に設定するともに、定期的な変更をお願いします。
c）また、ユーザー認証機能や PW 認証機能を備えている機器は積極的な利用を推奨します。

HITACHI

Inspire the Next