緊急のご案内（重要）第３報

2021 年 12 月 21 日
有限会社インターラック
代表：福田　匡
技術：江口　宏一朗

今年 4 月頃から、メーカーや機種に問わず**インターネットに接続**されている防犯カメラ用の録画装置（DVR）に対し、ネットワークを介し海外から**不正アクセス（サイバー攻撃）**が多く発生し様々な事象や障害が報告されております。

時間の経過と共に不正アクセスの手口も巧妙化し影響を受ける DVR メーカーと機種も増え続けており、11 月頃からは弊社の販売する **IRV シリーズでも確認**されております。

【対象機種】　2021/12/21　12:00 現在

IRV-HV8000 シリーズ（8004/8008/8016/8032）　**多く確認されています**
IRV-HD9000 シリーズ（9004/9008/9016/9032）　確認されていません
IRV-AT6000 シリーズ（6004/6008/6016）　調査調査中
IRV-A7000 シリーズ（7004/7008/7016）　調査調査中
IRV-AT6000N シリーズ（6004N/6008N）　調査調査中
IRV-A7000N シリーズ（7004N/7008N/7016N）　調査調査中
※いずれも**インターネットに接続され、DDNS（powerddns.com）を利用**しているもの

【主な事象】

① 遠隔（リモート）接続が重い、接続しづらい、接続できない、強制的に中断（切断）されるなど
② DVR が接続されているネットワーク（インターネット）の通信速度が遅い、繋がりにくい
③ 通信量（パケット量）が極端に増えている
④ ISP（プロバイダー）から警告及び注意などの書面（メール・電話）が届いている
⑤ 特定の IP アドレスに対し、通信を行っている
⑥ DVR が通常（これまで）とは違う動きをしたり動作が重い、突然停止する、突然再起動する、録画が停止するなど

【注意点①】　不正アクセス（サイバー攻撃）は**時間と共に手口が変わり巧妙化**していく為、現在までに確認されている上記の事象以外にも予想外な事が発生します。

【注意点②】　一般家庭や中小企業、大企業問わず不正アクセス（サイバー攻撃）は行われます。むしろセキュリティが強化されている大企業に比べ一般家庭や中小企業が攻撃され被害が出る事が多くあります。

【注意点③】　知らない所で気付かないうちに自らがマルウェア（ウイルス）等に感染し被害者となり、自らが不正アクセスを引き起こす加害者にもなる可能性があります。

【対応策】

第三者からの不正アクセス（サイバー攻撃）を受けない為の**最低限の自己防衛策**として

① **初期パスワードや簡単なパスワードでは使用しない。**ユーザー様ご自身で**パスワードを変更**して下さい。変更後のパスワードはユーザー様ご自身で保管し取り扱いには十分にご注意下さい。パスワード不明になった場合、現場での復旧は出来ません。メーカーでの有償修理預かりとなってしまいます。

② セキュリティ強化された**最新のファームウェア**を入手し **DVR をアップデート**する。
但し不正アクセスする側も更新された最新ファームウェアをも時間の経過と共に再び攻撃し突破する為、定期的に最新ファームウェアのリリース確認と更新は必要です。
最新ファームウェアは弊社ホームページをご確認頂くか、または担当営業よりご連絡ご提供させて頂きます。

③ **適切な手順で設定**を行って下さい。以下の手順は弊社の販売する IRV シリーズを例にした対応手順です。他社をご利用の場合は製品添付の取扱説明書（場合によっては CD-ROM に収録またはメーカーホームページからのダウンロードが必要）をご覧下さい。

【対応手順】

① DVR から **LAN ケーブルを外す**

② DVR の管理者（admin）の**パスワードを変更**する。

手順：メニュー ＞ 設定 ＞ システム ＞ ユーザー変更 ＞ admin ＞ パスワード変更

重要 user1～user14 を**使用している**場合はその**パスワードを変更**する

手順：メニュー ＞ 設定 ＞ システム ＞ ユーザー変更 ＞ user1～14 ＞ パスワード変更

重要 user1～user14 を**使用していない**場合は **user（ユーザー）を全て削除**する

手順：メニュー ＞ 設定 ＞ システム ＞ ユーザー削除 ＞ user1～14 ＞ 削除

③ 最新ファームウェアがある場合は**アップデート**する。ファームウェアのアップデート手順は以下をご覧下さい。

④ DVR を**再起動**する。（ファームウェアアップデートを行った際はアップデート実行中に再起動します）

⑤ ルーター（接続情報を持った大元となるルーター）を**再起動**する。
コンセントを抜いて 1 分ほどして差し直す事で再起動しますが、一時的にネットワーク（インターネット）が使用できなくなります。

⑥ DVR に **LAN ケーブルを接続**する。

【注意事項】

① パスワード変更に伴い、リモートソフト（NETUS-Pro）やスマートフォンアプリ（SmartEyes Pro）の**デバイス登録情報の変更**が必要となります

② ルーターのファームウェア更新が必要な場合があります。

③ １度不正アクセスを許してしまうと相手側に利用中の現在の IP アドレスが記録され、パスワードを変更しても攻撃は続く場合があります。その際 IP アドレスの変更が有効的な為、

ルーターの再起動が必要となります。

④　現在、この不正アクセス（サイバー攻撃）対応のセキュリティが強化された最新ファームウェアは**公開されていません。**

12 月 21 日午後 0 時現在、メーカーによって**開発中**です。

【最後に】

現在の所、今回の不正アクセス（サイバー攻撃）はユーザー様の個人情報や映像を抜き取ると言うものではなく、インターネットを介し海外から DVR に侵入し、DVR を介し国内または海外の別のネットワークに侵入する為の**踏み台**とされているケースです。また人の活動が少なくなり、すぐに異常を検知し対応する事が困難な**週末や深夜に活動**する点も確認されています。

侵入口は一般家庭や中小企業など小さくても、最終的には大きな所（大企業や政府、海外）を攻撃する事を目的としている場合がある為、攻撃を受けている側としては踏み台とされている一般家庭や中小企業から攻撃されているように見え誤解を受ける事もあります。

また通信回線がパンクするほどの大量のデータを意図的に送り付けてくる為、回線に余裕が無くなり他の通信に影響が出、大量の通信を行っているので ISP（プロバイダー）から「大量にやり取りをしている」と連絡が来てしまいます。

国をまたぎ世界規模に踏み台を作り大元となる真にはたどり着かないようになっており、対策を打ってもその上を行く技術で攻撃し、再び対策を打ってもまたそれを突破すると言ったのが繰り返されています。

ユーザー様に置かれましては、以上の対応手順を行って頂きますよう、お願い申し上げます。
また弊社では最新の情報をホームページ上でも随時公開しておりますので、ご覧下さい。

以上