弊社製 DVR における通信障害につきまして

㈱ファースト
福岡県福岡市南区市崎 1 丁目 2 番 41 号

近年、IoT 機器(ネットワークに接続する全ての物)を踏み台として利用するサイバー攻撃(DDoS 攻撃)を行う事象が全世界で増加傾向に有り、昨年辺りから FAX や DVR(録画機)等でも報告されています。
年々サイバー攻撃も手口が巧妙化し、影響を受ける機器も多岐にわたり、度々弊社 DVR でも確認されるようになりました。

主な症状と致しましては

・遠隔(リモート)が繋がらない、若しくは繋がりにくい
・インターネットの通信速度が遅い若しくは繋がらない
・DVR の動作が遅い
・DVR が勝手に再起動する

等です。
ISP(プロバイダ)からの確認の通知が来る事もあります。

動作自体はあくまでも、IoT 機器をサイバー攻撃の踏み台にするもので、現在の所この事象により映像や個人情報を盗む等の報告は上がっておりません。
しかしながら、気付かないうちに DVR が感染し、自らが知らないうちにサイバー攻撃を引き起こす加害者にもなる可能性もあります。
これらの不正アクセス(サイバー攻撃)を防ぐ為にはまず自己防衛が基本となります。

〈 確認機種 〉

・CFR-904E、CFR-908E、CFR-916E
・CFR-4EHD、CFR-8EHD、CFR-16EHD
・CFR-4EHA、CFR-8EHA、CFR-16EHA
・CFR-4EAAM、CFR-4EABC
・CFR-4EAA、CFR-8EAA、CFR-16EAA
・CFR-4EAB、CFR-8EAB、CFR-16EAB
・CFR-1004EA、CFR-1008EA、CFR-1016EA
・MD-404HD、MD-808HD
・MD-404HA、MD-808HA
・MD-404AA、MD-808AA
・MD-404AB、MD-808AB

〈 症状 〉

・ネットワーク通信速度が遅くなる
・プロバイダ等から通信量について通達が有る。
・リモート閲覧が出来ない、若しくは接続し辛い(Smart Eyes Pro、RMS、VMS)
等

〈 状況 〉

・DVR をインターネットに接続し、初期パスワードを使用している。
・DVR をインターネットに接続し、ウェブポートを使用している。

〈 原因 〉

IoT 機器※1 の脆弱性を狙った DDoS 攻撃(分散型サービス拒否攻撃)※2※3 により、DVR が踏み台となり、大量のパケット通信を行う事で、ネットワーク回線の帯域を専有しネットワーク機器が使用出来なくなる為。

(※1) IoT (Internet of Things):インターネットに接続し、情報をやり取りする機器。

(※2)Distributed Denial of Service 攻撃:ネットワークに接続する複数のコンピュータが特定のコンピュータに対して一斉に大量の通信を行うことで、サービスや機能を停止させようとする攻撃

(※3)DDoS 攻撃の対象は他に有り、IoT 機器はあくまでも踏み台

〈 対策 〉

この種のボットネットの特徴として、ネットワークをランダムで検索し、telnet 経由で他の IoT 機器へのログインを試み、感染を拡大して行く。ボットネット自体が機器へのログインの段階で、辞書攻撃と言うデフォルトで使用されている安易なパスワードを、総当たり攻撃により使用する為、下記対策を行って下さい。

・対策ファームウェアが用意されているものに対しては、ファームウェアの更新
　ファームウェアの更新方法及びダウンロードは弊社ホームページを参照して下さい。
※パスワードがデフォルトの場合、パスワードの変更が要求されます。
　要求がされない場合でも、出来る限り変更を行って下さい。
※変更したパスワードはメモ等をし、第三者の目に触れない様に大切に保管して下さい。
　パスワードを失念した場合は、弊社に返送後、有償にて出荷時の状態に初期化となります。その際に掛かる送料はお客様負担となりますので予め御了承下さい。

下記モデルは既にサポートが終了しており，対策版ファームウェアは提供されませんので、以下のワークアラウンドを実施して下さい。

・CFR-904E、CFR-908E、CFR-916E
・CFR-4EHD、CFR-8EHD、CFR-16EHD
・CFR-4EHA、CFR-8EHA、CFR-16EHA
・CFR-4EAAM
・CFR-4EAA、CFR-8EAA、CFR-16EAA
・MD-404HD、MD-808HD
・MD-404HA、MD-808HA
・MD-404AA、MD-808AA
・1stgen MD-404AB、1stgen MD-808AB

・当該機器をインターネットに接続せず、スタンドアロンで使用する
・パスワードを変更し、ルーター等の配下に DVR を接続した上でポート転送機能の設定を行い、WAN 側から機器の Web 管理画面（ウェブポート：80/tcp 番ポートなど）へのアクセスを遮断する
※ルーターの設定変更は間違えるとネットワーク障害が起きる可能性が有ります。設定を変更する際は、必ずネットワーク技術者が行って下さい。
・製品の買い替えを御検討ください

以上