

PDR, PNR シリーズ DVR をご使用中のお客様に大切なお知らせ

第2報

2021年5月25日

有限会社インターラック

技術担当：手束浩二

お客様各位

日頃より、弊社防犯機器をご愛用いただきまして、誠にありがとうございます。

2021年5月7日頃より、PDRシリーズのデジタルビデオレコーダ（以降「DVR」と記述します）をインターネットに接続して使用中のお客様において、お客様が使用中のDVRに対してインターネットを介した海外からの不正アクセスが確認されている件について、弊社において独自に調査した結果を踏まえて、改めて不正アクセス対策のご確認をお願い致します。

お客様へのお願い

DVRの動作に異常がない場合

① **重要** 必ずお客様自身のパスワードを設定してください。

お客様におかれましては、**デジタルビデオレコーダ、ネットワークビデオレコーダ、IPカメラ等の管理者パスワードが初期設定のままになっていないか今一度ご確認をお願い致します。万一初期設定のままになっている場合は、大至急お客様自身の“他人にわからない”パスワード（数字とアルファベットを含む8文字以上を推薦）に変更していただきますよう強くお願い致します。**

また、パスワード変更後は、パスワードを変更した機器を念のため再起動してください。

なお、**管理者パスワードを変更する代わりに管理者ユーザー名を変更する対処法は絶対に避けてください。**（対策の効果が期待出来ません。）

The screenshot shows the 'システム' (System) settings page, specifically the 'ユーザーアカウント' (User Account) section. The interface is in Japanese. The '管理者' (Administrator) user is selected. The 'パスワード' (Password) field is highlighted with a yellow box, and the 'カスタム P/W' (Custom P/W) option is selected. The '保存' (Save) button is highlighted with a yellow box. Four callout boxes provide instructions: (1) Select '管理者' (Administrator), (2) Select 'カスタム P/W' (Custom P/W), (3) Enter the password, and (4) Save the change. A pink callout box notes that simply changing the password field without saving is ineffective.

(1) 「管理者」を選択する

ここを変更するだけでは効果無し

(2) 「カスタム P/W」を選択する

(3) パスワードを入力する

(4) 変更を保存する

DVRが既にフリーズしていて操作が出来ない場合

① DVRからLANケーブルを抜いてください。

② DVRの電源を一度切ってから入れ直してください。

③ **重要** 必ずお客様自身のパスワードを設定してください。

お客様におかれましては、**デジタルビデオレコーダ、ネットワークビデオレコーダ、IPカメラ等の**

管理者パスワードが初期設定のままになっていないか今一度ご確認をお願いいたします。万一初期設定のままになっている場合は、大至急お客様自身の“他人にわからない”パスワード（数字とアルファベットを含む8文字以上を推薦）に変更していただきますよう強くお願い致します。

また、パスワード変更後は、パスワードを変更した機器を念のため再起動してください。

なお、**管理者パスワードを変更する代わりに管理者ユーザー名を変更する対処法は絶対に避けてください。**（対策の効果が期待出来ません。）

- ④ 可能ならば DVR の録画用 HDD をフォーマットしてください。
一度不正アクセスを受けてフリーズした DVR は、録画用 HDD のデータが壊れていたり不要なデータが書き込まれていたりする可能性があります。念のため録画用 HDD をフォーマットしていただく事をお勧めします。
- ⑤ 必要に応じてルータを再起動してください
不正アクセスを受けた直後は、パスワード変更をした後であっても、攻撃元から繰り返し不正なアクセスを試みられる場合があります。ルータを再起動する事でグローバル IP アドレスが変更されることによって、不要な接続要求を回避できる可能性があります。
- ⑥ 必要に応じてルータの packets フィルタを設定してください
不正アクセスを受けた直後は、パスワード変更をした後であっても、攻撃元から繰り返し不正なアクセスを試みられる場合があります。フリーズが発生する場合は、レコーダのログを確認していただき、身に覚えのない特定の IP アドレスからの「接続」や「切断」が記録されている場合には、ルータの packets フィルタを使用する等して、特定の IP アドレスからのアクセスを遮断していただく方法も一定の効果が期待出来ます。
- ⑦ DVR に LAN ケーブルを接続してください。



管理者パスワードを変更する代わりに管理者ユーザー名を変更してはいけない理由

今回の不正アクセス事案では、メーカーがサービス用に使用するための特別なアカウントが悪用されており、この特別なアカウントは管理者とパスワードを共有しております。このパスワード共有の仕組みは、たとえメーカーのサービス担当者であっても、お客様がパスワードを変更した後は DVR にアクセス出来ないようにする事を保証するためのものです。

つまり、今回の事案では、管理者ユーザー名を変更するだけでは、サービス用アカウントのユーザー名とパスワードが変更されないため、不正アクセスを許してしまう事になります。