令和５年３月 28 日
警　　察　　庁

家庭用ルーターの不正利用に関する注意喚起について

サイバー攻撃事案の捜査の過程で、家庭用ルーター（以下「ルーター」という。）がサイバー攻撃に悪用され、従来の対策のみでは対応できないことが判明したことから、警察では、複数の関係メーカーと協力し、官民一体となって注意喚起いたします。

１　使用された手法

今回確認された手法は、一般家庭で利用されているルーターを、サイバー攻撃者が外部から不正に操作して搭載機能を有効化するもので、一度設定を変更されると**従来の対策のみでは不正な状態は解消されず、永続的に不正利用可能な状態となってしまう**手法です。

２　推奨する対応

従来の対策である

- ○　初期設定の単純な ID やパスワードは変更する。
- ○　常に最新のファームウェアを使用する。
- ○　サポートが終了したルーターは買換えを検討する。

に加え、**新たな対策として**、

- ○　**見覚えのない設定変更がなされていないか定期的に確認する**。

をお願いします。

具体的には、ルーターの管理画面で次の事項を定期的に確認し、問題があった場合には、その都度是正するようお願いします。

(1)　見覚えのない**「VPN 機能設定」や「DDNS 機能設定」、「インターネット（外部）からルーターの管理画面への接続設定」の有効化がされていないか**確認する。

(2)　VPN 機能設定に**見覚えのない VPN アカウントが追加されていないか**確認する。

(3)　**見覚えのない設定があった場合**、**ルーターの初期化**を行い、**ファームウェアを最新に更新**した上、**機器のパスワードを複雑なものに変更**する。

※　ルーターの設定の詳細については、取扱説明書やメーカーのホームページを確認してください。

また、メーカーのサポートが終了したルーターは、機器の脆弱性を改善するためのファームウェアの更新が行われず、さらにセキュリティのリスクが高まるので、買換えの検討をお願いします。