

【注意喚起】

Mirai 亜種の感染活動に関する注意喚起について

外部セキュリティ機関より、2017年11月頃より、国内においてMirai

(※)の亜種による感染活動が確認されている旨の情報を入手しましたので、注意喚起を行います。Miraiやその亜種のマルウェアに感染した機器は、ボットネットに取り込まれ、攻撃者によりDDoS攻撃などに悪用される可能性があります。国内での感染事例が増加しており、早急な対策が必要なことから、該当するIoT機器の利用状況および対応状況についてご確認ください。対策として、機器ベンダによるファームウェアの修正バージョンが公開されている場合は、アップデート等の処置をご検討ください。また、ファイアウォール等で機器へのアクセスが制限されていることや、機器に適切なパスワードが設定され認証機能が有効になっていること等をご確認ください。

○参考

IoT製品の脆弱性を悪用して感染を広げるMiraiの亜種に関する活動(2017-12-19)

http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf

Mirai 亜種の感染活動に関する注意喚起

<https://www.jpccert.or.jp/at/2017/at170049.html>

脆弱性が存在するルータを標的とした宛先ポート52869/TCPに対するアクセス及び日本国内からのTelnetによる探索を実施するアクセスの観測等について

<https://www.npa.go.jp/cyberpolice/detect/pdf/201712191.pdf>

※：ルータ、監視カメラ、ストレージ機器や特定産業向け組み込み通信機器などのIoT機器を標的としたマルウェア

【問い合わせ先】

文部科学省大臣官房政策課情報システム企画室情報セキュリティ係・情報監理係

〒100-8959 東京都千代田区霞が関3-2-2

TEL: 03-5253-4111 (内線 2248、3040、3060)

E-mail: seijoho@mext.go.jp<mailto:seijoho@mext.go.jp>