# Article information:

警視庁が家庭用ルーターの不正利用に注意喚起。従来の対策では防げないサイバー攻撃を確認（PHILE WEB） - Yahoo!ニュース  
<https://news.yahoo.co.jp/articles/dbce89c499615eff627ec21dee024bb12df86c0b>

# Article summary:

1. The Metropolitan Police Department in Japan has issued a warning about the illegal use of home routers for cyberattacks.

2. Conventional countermeasures are not enough to deal with this problem, and a public-private partnership alert has been issued.

3. The police recommend regularly checking router settings for unfamiliar changes, and manufacturers such as IO data devices and ELECOM have expressed their support for the alert.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article reports on the Metropolitan Police Department's warning about the use of home routers for cyberattacks. The police found that conventional countermeasures were not enough to deal with the problem, and a public-private partnership alert was issued. The article provides some details on the method used by cyber attackers, which involves illegally operating a router from outside to activate installed functions. Once settings are changed, fraudulent states cannot be resolved with conventional countermeasures alone.

The article suggests that users should regularly check whether unfamiliar settings have been changed and lists specific settings to check. If there is an unfamiliar setting, users should initialize the router, update firmware to the latest version, change passwords to complicated ones, etc. The article also recommends replacing routers for which manufacturer support has ended.

The article mentions IO data devices and ELECOM expressing their support for the alert and being members of the Digital Life Promotion Association (DLPA). ASUS also expresses its support and uses AiProtection attached to its router.

Overall, the article provides useful information on how to prevent home routers from being used for cyberattacks. However, it lacks some important details that could help readers better understand the issue. For example, it does not explain how cyber attackers can illegally operate a router from outside or what specific functions they activate once they gain access.

Additionally, while the article mentions DLPA-recommended Wi-Fi routers with enhanced security features, it does not provide any evidence or explanation as to why these routers are more secure than others. This lack of evidence raises questions about potential biases towards DLPA-recommended products.

Furthermore, while the article notes that manufacturers expressed their support for the alert and recommended products with enhanced security features, it does not mention any potential conflicts of interest or promotional content in this regard.

In terms of bias and one-sided reporting, the article only presents one perspective on home router security without exploring any counterarguments or alternative solutions. It also does not present both sides equally, as it focuses more on the police's warning and recommended countermeasures than on potential risks or limitations of these measures.

In conclusion, while the article provides some useful information on home router security, it lacks important details and evidence, potentially biases towards DLPA-recommended products, and presents a one-sided perspective without exploring alternative solutions or potential risks.

# Topics for further research:

* How do cyber attackers illegally operate home routers from outside?
* What specific functions can cyber attackers activate once they gain access to a home router?
* What are the potential risks and limitations of the recommended countermeasures for home router security?
* Are DLPA-recommended Wi-Fi routers really more secure than other routers
* and if so
* why?
* Are there any conflicts of interest or promotional content involved in the manufacturers' support for the alert and recommended products?
* What are some alternative solutions for preventing home routers from being used for cyberattacks?

# Report location:

<https://www.fullpicture.app/item/f497153f00928d84275297e6d18d8716>