MITSUBISHI ELECTRIC

TECHNICAL BULLETIN

FA-A-0305-B

Precautions When the Modules With the Ethernet Port are Used

■Date of Issue

July 2020

■Relevant Models

MELSEC iQ-R, MELSEC iQ-F, or MELSEC-Q/L/F series modules with an Ethernet port

Thank you for your continued support of Mitsubishi Electric programmable controllers.

We will inform you of the measures that must be taken by you and the precautions when a module with an Ethernet port*1 is used.

*1 A module with an Ethernet connector

1 OVERVIEW

Relevant models

MELSEC iQ-R, MELSEC iQ-F, or MELSEC-Q/L/F series modules with an Ethernet port

Description

When relevant models are directly connected to networks without firewall protection, the models may be subjected to cyber attack including unauthorized access or denial-of-service (DoS) or the communication data may be tapped or tampered with via networks.

Take measures described in the next chapter.

2 MEASURES TAKEN BY USERS

Take the following measures against cyber attack including unauthorized access or denial-of-service (DoS) and against tapping or tampering with communication data via networks.

Item	Description
Checking for network connection	Check whether the modules installed on any used equipment are connected to a network or not.
Checking for firewalls	Block access from communications via untrusted networks and hosts using firewalls.
Installation of a VPN	Block access from communications via untrusted networks and hosts by encrypting communication routes with a VPN.

Contact your IT department or local supplier whether your modules are connected to networks or not, and whether measures such as firewalls and a VPN are taken or not.

REVISIONS

Version	Date of Issue	Revision
A	May 2020	First edition
B	July 2020	Correction of words to support vulnerabilities