Think Automation and beyond...

Security Notes

In proportion to the recent rapid development of the Internet society, the importance of ensuring the security in networks is increasing. Therefore, we would like to inform you of the following security precautions that must be taken when using our products. We ask that you understand these precautions before using our products.

Security Notes

In general, if a network is built without proper security-related measures, the following problems may occur:

- ✓ System shutdown, unauthorized operation, exploitation of confidential information, falsification or destruction of data, or malware infection may occur due to unauthorized intrusion from an external network
- ✓ Being used as a stepping stone by a malware infection, turning from a victim to a perpetrator and attacking other network devices
- ✓ Unexpected information leaks or spills as a result of allowing network services
- ✓ Unauthorized operation by spoofing
- ✓ Secondary damages, such as injury, compensation for damages, reputational damage, opportunity loss, may be caused by the above problems

To prevent the above problems, refer to the security countermeasure examples described below and properly configure our products, other devices in the same network, and the security functions that those devices support, and then connect our products to the network. If necessary, take additional measures that are sufficient to avoid possible security risks.

Do not directly connect our products to the communication lines of telecommunication carriers (mobile communication companies, fixed-line communication companies, Internet providers, etc.) or the public wireless LAN. When connecting our products to the Internet, be sure to do so through a router or similar device.

New means of unauthorized access and control system vulnerabilities are constantly being discovered, and no matter how many security measures are implemented, security risks remain. We strongly recommend that you understand that network connections are always risky and that you always keep up with new information and take necessary security measures.

Please note that we are not responsible for any loss, damage, or other expenses incurred directly or indirectly as a result of unauthorized access.

Examples of security measures

Building a Closed Network and Encryption

When connecting a local area network where our products exist to an external network, use a closed network such as a dedicated network or VPN. Apply measures such as encryption (SSL/TLS) whenever possible. Even if the network is built using a closed network, the security may be breached by special methods and such risk should be considered.

Passwords

Refer to the following points when you set password. For details on how to set the passwords for our products, refer to the user's manual corresponding to each product.

- ✓ Change from the default password
- ✓ Use a strong password that is difficult to guess. A password should contain large and small letters, numbers, etc., and its length should be long.
- ✓ Change the password periodically and manage it securely.

Access restrictions

Refer to the following points and set access restrictions for devices connected to the network. For the setting method of our products, refer to the user's manual corresponding to each product.

- ✓ Stop unnecessary network services and ports.
- ✓ Allow connections only from specific access sources.
- ✓ Restrict access rights per account.

Other reference information

Various information on security has been published in various countries, so please refer to them when building and operating your network.