WHITE PAPER

Secure communication

- Security functions of i-PRO system –

Panasonic Video surveillance systems

Table of Contents

1. Introduction

Cyber-attacks on IoT devices have been increasing in recent years. Surveillance systems centering on analog cameras and recorders had mainly been used in closed networks such as companies' internal networks. However, with the migration of surveillance camera systems from analog to digital, network composition is becoming large scale and being connected to the Internet is becoming the norm. Moreover, surveillance systems are recognized as being an important part of the social infrastructure, and the risk of cyber-attacks on IoT devices is similarly increasing day by day.

This white paper describes the functions of and how to set security functions on Panasonic's i-PRO series of surveillance cameras and recorders (hereinafter, the "i-PRO system")

2. Outline

Measures against security threats need to take into account the environment of the system, assets to protect, and what the information is.

The following steps are ordinarily taken when considering cyber security of surveillance camera systems.

Step 1: Identify the overall composition of the surveillance camera system to protect.

Step 2: Identify information, functions and assets to protect on the system.

Step 3: Identify presumed threats to information, functions and assets to protect (threat analysis).

Step 4: Identify best practices in measures to counter threats.

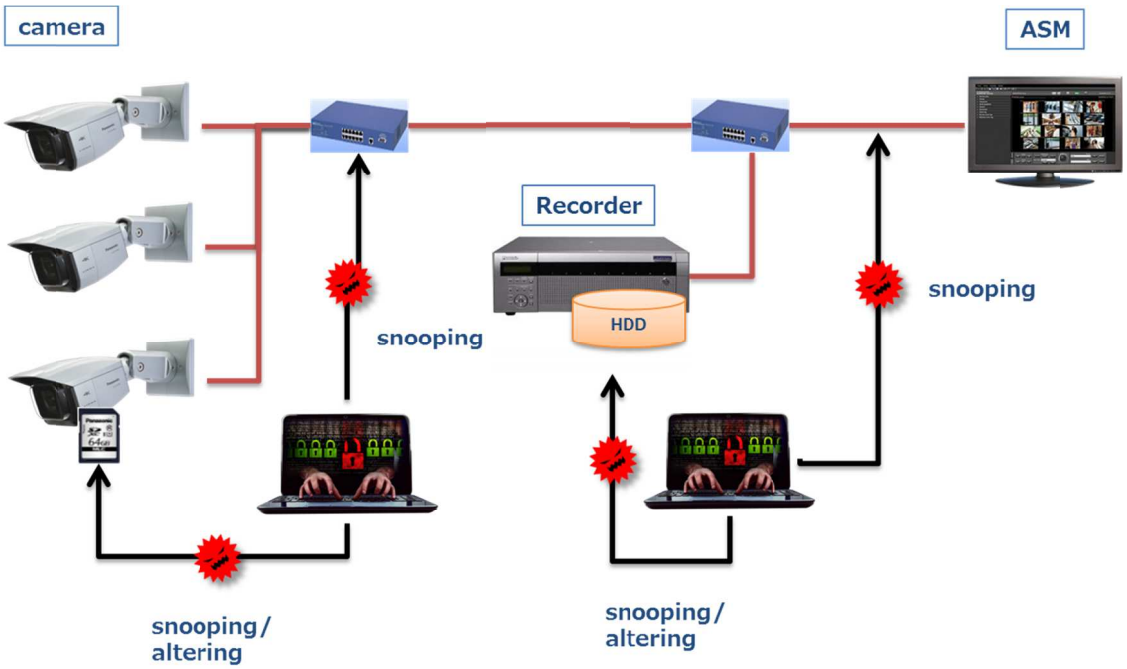
Step 5: Select measures to take considering threat level, damage level, costs, etc.

This white paper covers the security functions held by the i-PRO series in the following chapters, but implementing all of those may prevent the desired functionality from being exhibited or decrease ease of use. You should take sufficient measures upon thoroughly analyzing threats.

3. Common security functions of the i-PRO series

3.1. Functions and the areas that they protect

The diagram shows a system using common surveillance cameras. As shown in the figure, there are a variety of risks, and cyber attackers aim for the weakest part of the system. Therefore, measures need to be taken for all parts where it is judged through threat analysis that vulnerabilities are present.



Individual threats and effective countermeasures are shown in the table below.

Threat	Countermeasure
Access by unauthorized client	Authentication by password
	Host authentication
	Deactivation of unnecessary services
	802.1X
Snooping/alteration on network	Communications encryption (HTTPS)
Alteration of recorded data	Data encryption
Alteration of recorded data	Detection of recording alteration

3.2. User name and password

The most basic method of preventing unauthorized access to surveillance equipment is to set a user name and password to restrict access. A default account name and password are set when shipping from the factory, and some devices have a user account embedded that cannot be changed. Also, some devices can be accessed without a password (no need for authentication) by default. If a default password is set, this provides the benefit of being able to start using the device right away, but the password can be obtained by anyone by searching the Internet or from the device's instruction manual. Also, cyber attackers are in possession of simple user account names and passwords (root/12345, etc.) set by default and make unauthorized access by those. i-PRO series cameras (version xxx or later) and recorders do not have a user account name or password set by default, and use of a default password is prohibited by setting those at time of first access.

Caution is also needed regarding the user account privileges set here. All device settings, operations, and the like can be made if administrator privileges are granted, so whether or not administrator privileges are needed for the account that is added needs to be considered when registering it.

If a password operation policy is decided by the organization you belong to, it is best to adhere to that. If one is not decided, the following policy is recommended.

- Use two or more types of characters (letters, numbers, symbols) for the password.
- Change the password periodically.

3.3. Digest authentication

Even if use of an appropriate user account name and password are required, network capturing by a cyber attacker may enable those to be illicitly obtained depending on the authentication method.

The following two authentication methods are defined for HTTP.

① Basic authentication

With basic authentication, user name and password are sent as plain text. For that reason, it must not be used unless absolutely necessary to maintain backward compatibility.

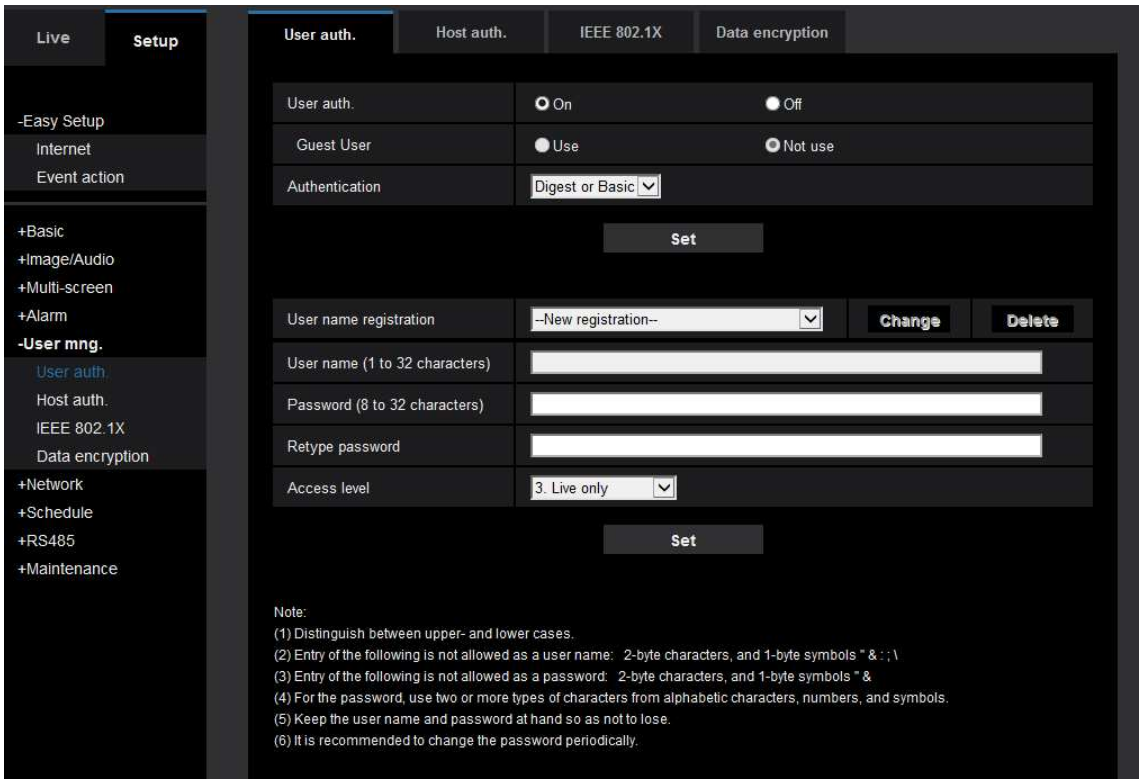
② Digest authentication

With digest authentication, user name and password are sent hashed by MD5. It is difficult to restore hashed values to their original text strings, so snooping on and alteration of user names and passwords can be prevented. Here, anyone can request the hash value from an ID and password, so

if frequently used combinations (such as user name: root, password: 12345) are used, they can be easily guessed. For reasons such as this, frequently used passwords must not be used.

With i-PRO cameras, either authentication is accepted by default in accordance with a request from the client connecting. To set so only digest authentication is accepted, select [Setup] -> [User mng.] -> [User auth.] and set [Authentication] to Digest.

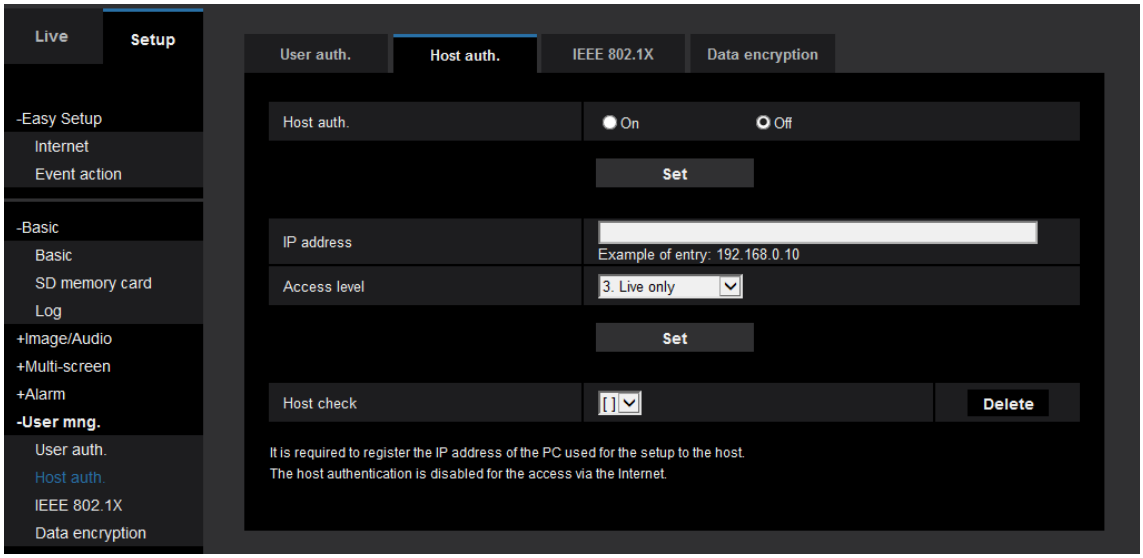
(Settings page capture)



3.4. IP address filter (host authentication)

If the IP address or network that the client accessing an i-PRO camera belongs to is decided, access from networks other than that can be blocked by setting an IP address filter (host authentication).

This can be set from the browser at [Setup] -> [User mng.] -> [Host auth.].



To authorize only a specific IP address, input an address like 192.168.0.100. To authorize access only the network that the client belongs to, entering a subnet by CIDR notation like 192.168.0.0/24 authorizes access from the entire subnet.

When setting, it is important to carefully confirm that there are no mistakes in the range that is allowed access. If mistakes are made in setting and the camera cannot be accessed, it will need to be reset to factory default.

Even if performing IP address filtering with IPv6 activated, one must note that access can be made from IPv6 addresses.

3.5. Deactivation of unnecessary services

A cyber attacker can use services that are active on a device as a platform for attacks. Especially if telnet service is activated, there is risk of the root account being taken over by entering a password and the device being infiltrated. Settings for the device may be changed or internal information taken, or it may be used as a platform for attacking other devices by setting a malware. With i-PRO cameras, infiltration of the device is prevented by deactivating default services. Only the following services are active by default with the i-PRO system.

- HTTP (80)
- RTSP (554)

3.6. IEEE 802.1x

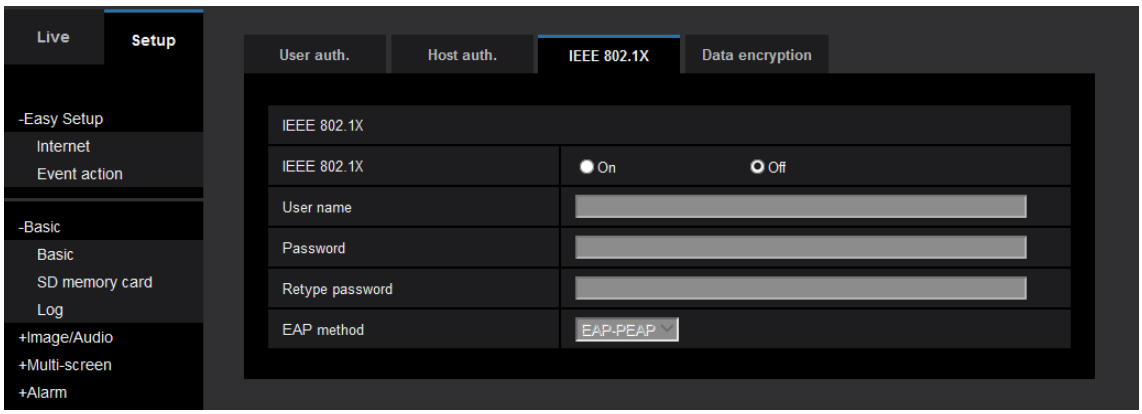
IEEE 802.1x is technology that uses a LAN switch to make so only approved devices can make a network connection. By using this mechanism, malicious entities can be prevented from connecting a PC to an open switching hub port on the LAN to infiltrate the network and make unauthorized access or snoop.

With IEEE 802.1x, software called a supplicant must be installed on the client PC attempting to access and an authentication LAN switch and authentication service must be readied. A client that wants to access first makes a request to connect to the authentication LAN switch and sends an EAP (Extensible Authentication Protocol) message. The authentication LAN switch forwards the EAP message to the authentication server, and the server judges whether or not to allow a connection.

There are different types of EAP, including EAP-MD5, PEAP, and EAP-TLS. EAP-MD5 and PEAP are methods of authentication by ID and password, and EAP-TLS uses digital certificates for authentication.

Currently (as of February 2017), only some i-PRO series cameras support IEEE 802.1x, with only EAP-MD5 and PEAP supported as the EAP; however, applicable models and authentication methods will be expanded in the future.

Camera settings can be configured from [Setup] -> [User mng.] -> [IEEE 802.1x] tab.



3.7. HTTPS

HTTPS (Hyper Transfer Protocol Secure) is a protocol to make secure communications by HTTP, and it makes HTTP communications on secure connections provided by SSL/TLS protocols.

Two major effects can be gained by using HTTPS.

① Prevention of snooping

Communications is encrypted by using HTTPS, and even if data is obtained on the network, it is rendered unreadable. By using this technology, snooping can be prevented.

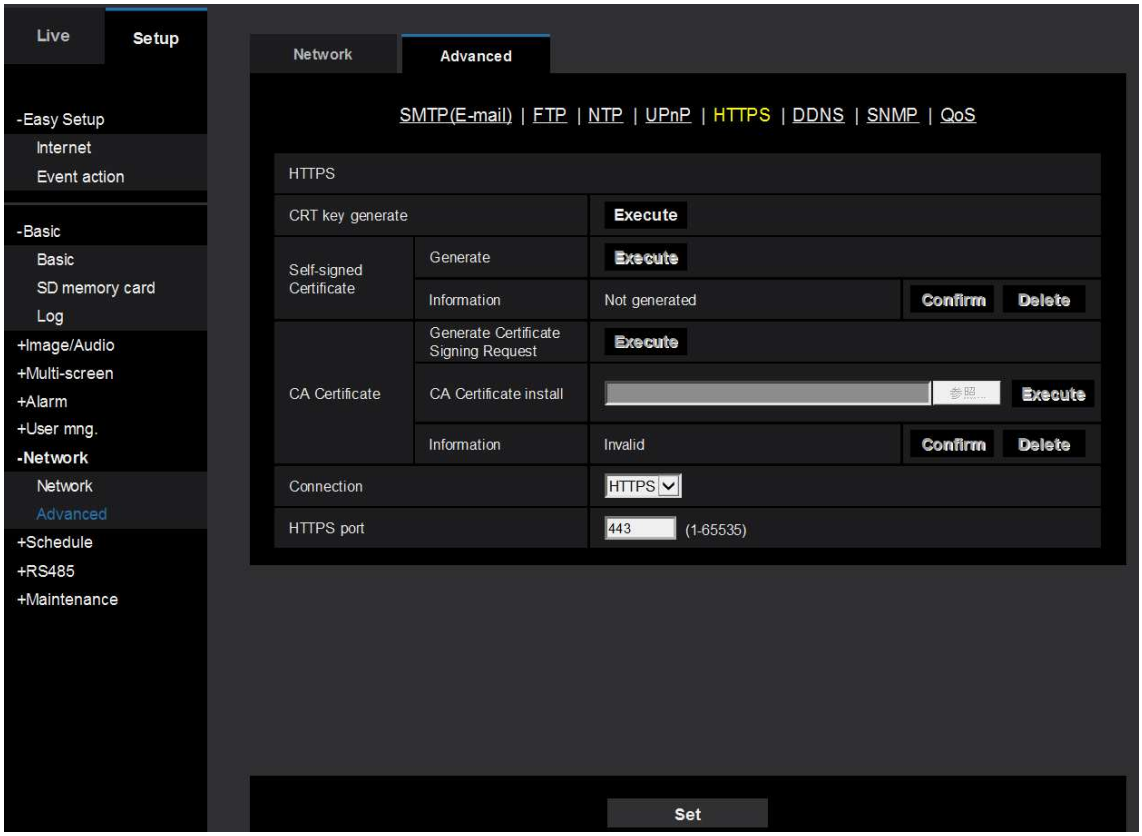
To encrypt communications by HTTPS, a specific secret key must be held in the camera/recorder. For that reason, a secret key generated outside is ordinarily imported to the camera or each camera is accessed individually when set up and a specific secret key needs to be generated. In the former method, there is a possibility of the secret key being leaked when importing. And in the latter, it takes time to generate in the camera a secret key with sufficient encryption strength, making it very exhausting work in an environment with many cameras/recorders set up.

Panasonic was the first in the world to provide products where a secret key and digital certificate are preinstalled, starting with some cameras (as of April 2016, surveyed by Panasonic). This work is done in a strictly controlled factory, and the certificate authority issuing (signing) certificates is controlled by a world-famous security vendor with a high level of security.

② Preventing spoofing

Spoofing involves using a forged PC or camera and pretending to be the camera/recorder the user is trying to access to exploit passwords and other information. This is a method often used in phishing of online banking and the like. In order to prevent spoofing, the identity of the digital certificate sent from the connecting device (camera/recorder) must be verified when establishing HTTPS communications. Specifically, the issuer (signer) of the digital certificate must be trusted by the connecting device (client). With cameras of many vendors, a function to generate self-signed certificates is provided as a method where HTTPS communications can be made temporarily; but with self-signed certificates, one issues certificates one's self, so the objective level of trust is low. As an analogy, this is like presenting a self-made passport at the immigration area of an airport. With preinstalled certificates used by Panasonic, a certificate authority that generates certificates is managed by world-famous and highly trusted security vendor as previously mentioned, so the possibility of forged certificates being used is extremely small.

HTTPS settings can be changed by opening [Setup] -> [Network] -> [Advanced] tab -> [HTTPS] page, changing [Connection] to [HTTPS] and pressing the [Set] button.



The preinstalled certificates are signed by a private CA, and a root certificate must be installed and registered on the client PC in order to confirm the signer to prevent spoofing. See the instruction manual for details.

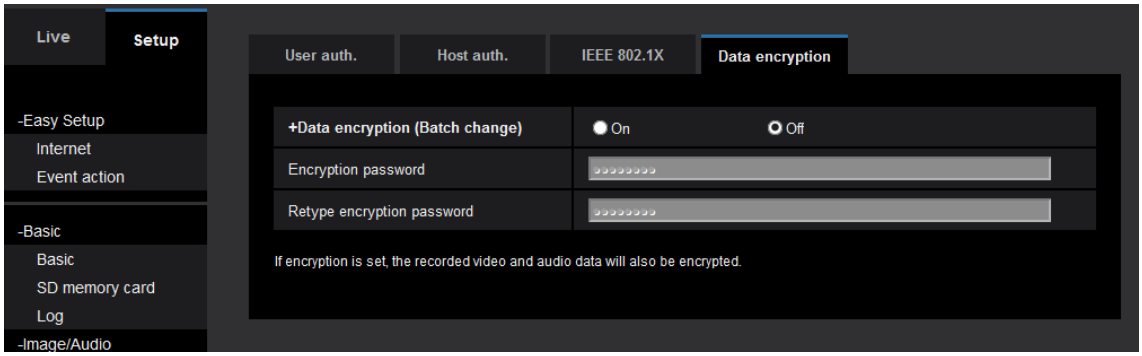
3.8. Data encryption

Data encryption, unlike HTTPS and VPN, involves encrypting video and audio data only. HTTPS and VPN encrypt the communications path, so data after communications is decrypted and recorded. If recorded data is leaked, it will be in a state where it can be viewed. With data encryption, however, it is the data that is encrypted, so it remains encrypted even recoded to storage. Thus, even if the hard drive or SD card is stolen or data on the cloud is leaked, video cannot be peeked at.

There is no industry standard method of data encryption, and the system as a whole needs to handle data encryption to execute it.

Currently (as of February 2017), some models in the i-PRO series (cameras, recorders, PC software) handle data encryption.

Camera settings can be configured from [Setup] -> [User mng.] -> [Data encryption] tab.



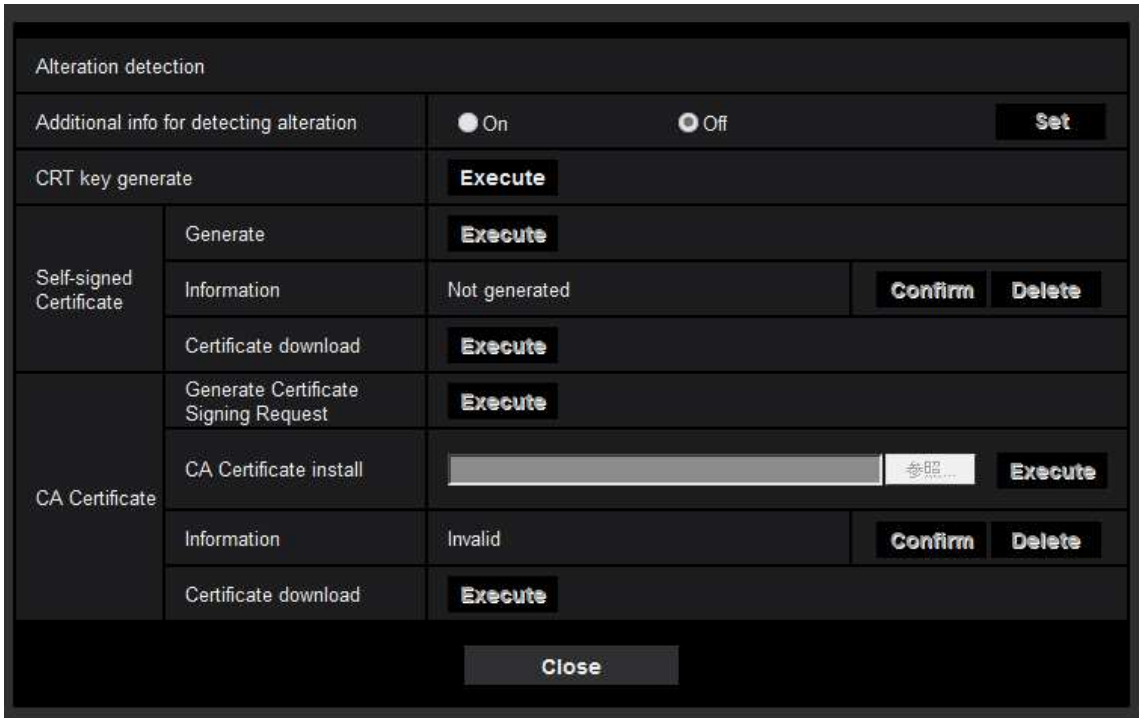
3.9. Alteration detection

There is a risk of data recoded on storage being moved somewhere else. If sent by email or carried on an SD card, there is a possibility of data being altered or replaced on the transport route. The alteration detection function detects when such risks occur.

Specifically, the hash value of video data is calculated while shooting, encrypted using the secret key preinstalled on the camera, and added to recoding data in advance. That encrypted data is called a "signature". When detecting presence of alteration, the hash value of video data is calculated again; and if that value is confirmed to be the same as the hash value decoded with the certificate of the camera used for shooting, it can be certified that the data has not been altered.

The signature created by the camera's secret key can only be decrypted with the public key included in the camera's certificate. As covered in the section on HTTPS, it cannot be objectively confirmed who signed with a self-signed certificate. For example, if data carried on an SD card is signed after falling into the hands of someone with malicious intent and is altered, that alteration cannot be detected. In order to prevent such situations, a certificate preinstalled on the device itself must be used.

Settings can be configured by opening a separate window by selecting [Setup] -> [Basic] -> [SD memory card] tab -> [Alteration detection], turning [additional info for detection alteration] to [On] and pressing the [Set] button.



Alteration detection only handles movies (MP4 format), and confirmation can be made by dedicated software.

3.10. Vulnerability testing

Software installed on network devices has undergone many cyber-attacks in the past, and many vulnerabilities have been found. As a countermeasure against that, vulnerabilities found in the past have been compiled in a CVE (Common Vulnerabilities and Exposures) database, and that has been shared worldwide. Also, attacks are made on past vulnerabilities based on this disclosed database.

The i-PRO series has undergone verification testing on vulnerabilities registered to the CVE, and appropriate countermeasures are taken for vulnerabilities discovered. With this effort, the threat of cyber attacks on known problems can be reduced. Moreover, with the i-PRO system, module structure is identified using our own modules in HTTPS communications as well, and we take our own countermeasures against vulnerabilities. And encryption algorithms with weak security, such as SSL3.0 and RC4, are not used.

There is also the possibility that vulnerabilities not known at present too may be found in the future. Panasonic is constantly monitoring for new vulnerabilities, and actions are taken promptly when it is judged that countermeasures are needed. In order to protect yourself from the latest cyber attacks, it is recommended that you check the Panasonic website periodically and always update to the latest firmware.

3.11. Firmware

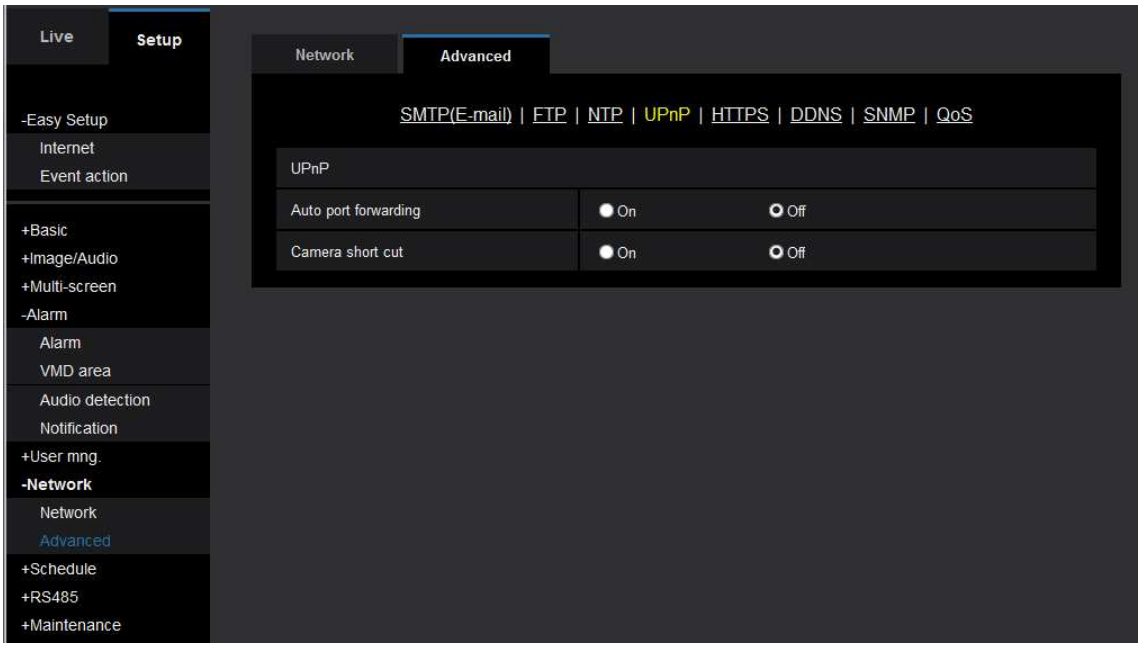
There is risk in the firmware data itself as well. There is a possibility of being attracted to spoofing sites by targeted attack email and firmware being updated with a version that includes a virus, so firmware must always be downloaded from the vendor's page.

If the firmware posted is not encrypted, there is a risk of it being analyzed by persons with malicious intent, vulnerabilities being detected, and attacks being made. There have been cases where a device is attacked by firmware vulnerabilities even if there are no problems with the user's settings, rendering it inoperable, and DDoS attacks being made on other servers via the device. With i-PRO cameras and recorders, all firmware is securely encrypted and it cannot be analyzed.

4. Cautions with network cameras

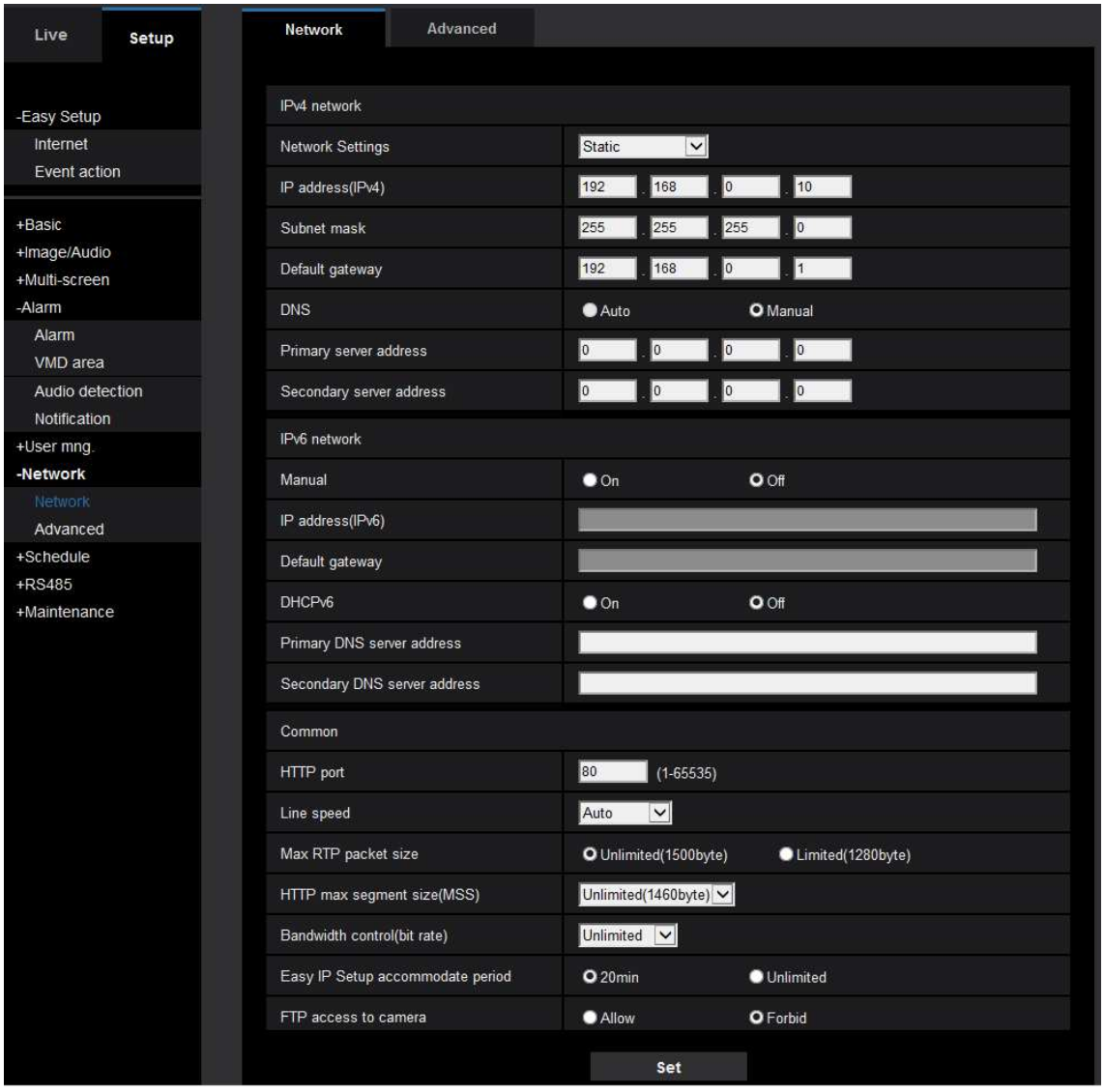
4.1. UPnP

Configuring UPnP automatic port forwarding settings, port forwarding settings are made for NAT routers and network cameras can be accessed from the Internet outside the network holding the cameras. To reject access from outside, the Auto port forwarding setting on the UPnP settings screen must be turned off.



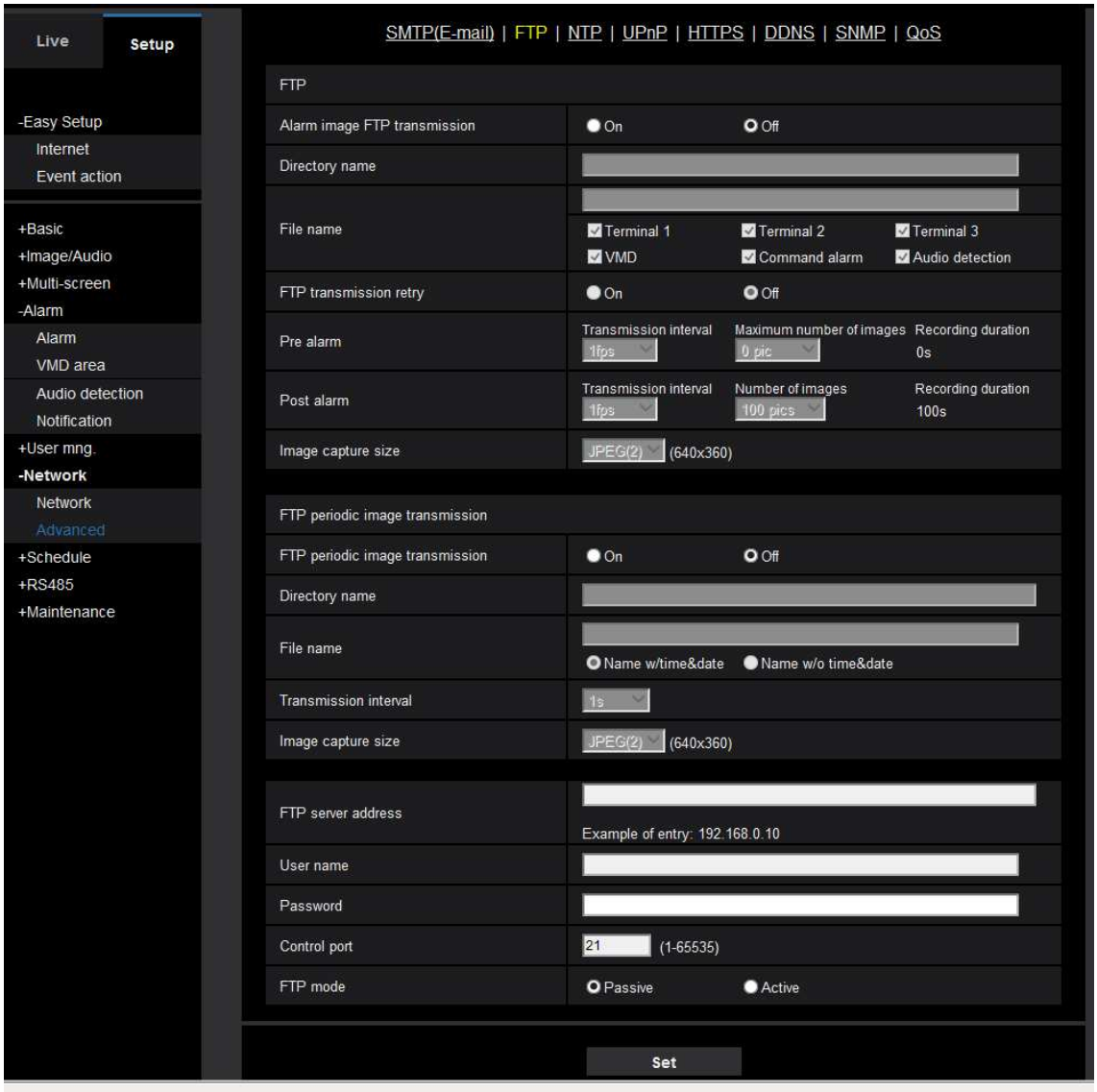
4.2. FTP servers

By activating the FTP server function, network cameras can be accessed from FTP clients by FTP. FTP communications is not encrypted, so it is recommended that the FTP server function be turned off when not using an FTP server function in order to prevent snooping on IDs, passwords, and transferred data. The FTP server function can be turned off by setting the FTP access to camera setting on the Network settings screen to Forbid.



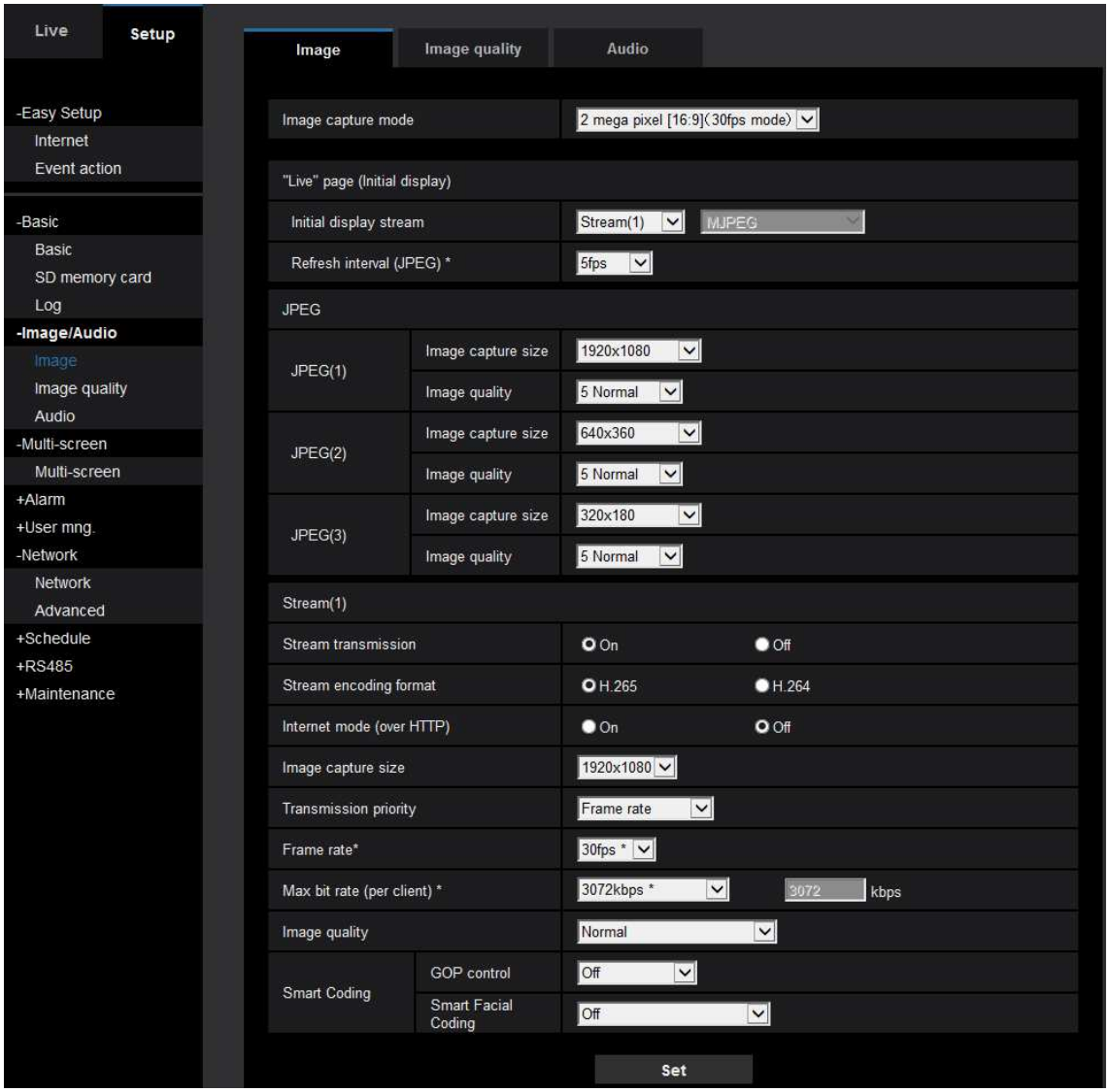
4.3. FTP client

By activating the FTP client function, FTP image files can be transferred to an external FTP server. FTP communications are also not encrypted, so it is recommended that the FTP client function be turned off when using in an unsecured environment in order to prevent snooping on IDs, passwords and transferred data.



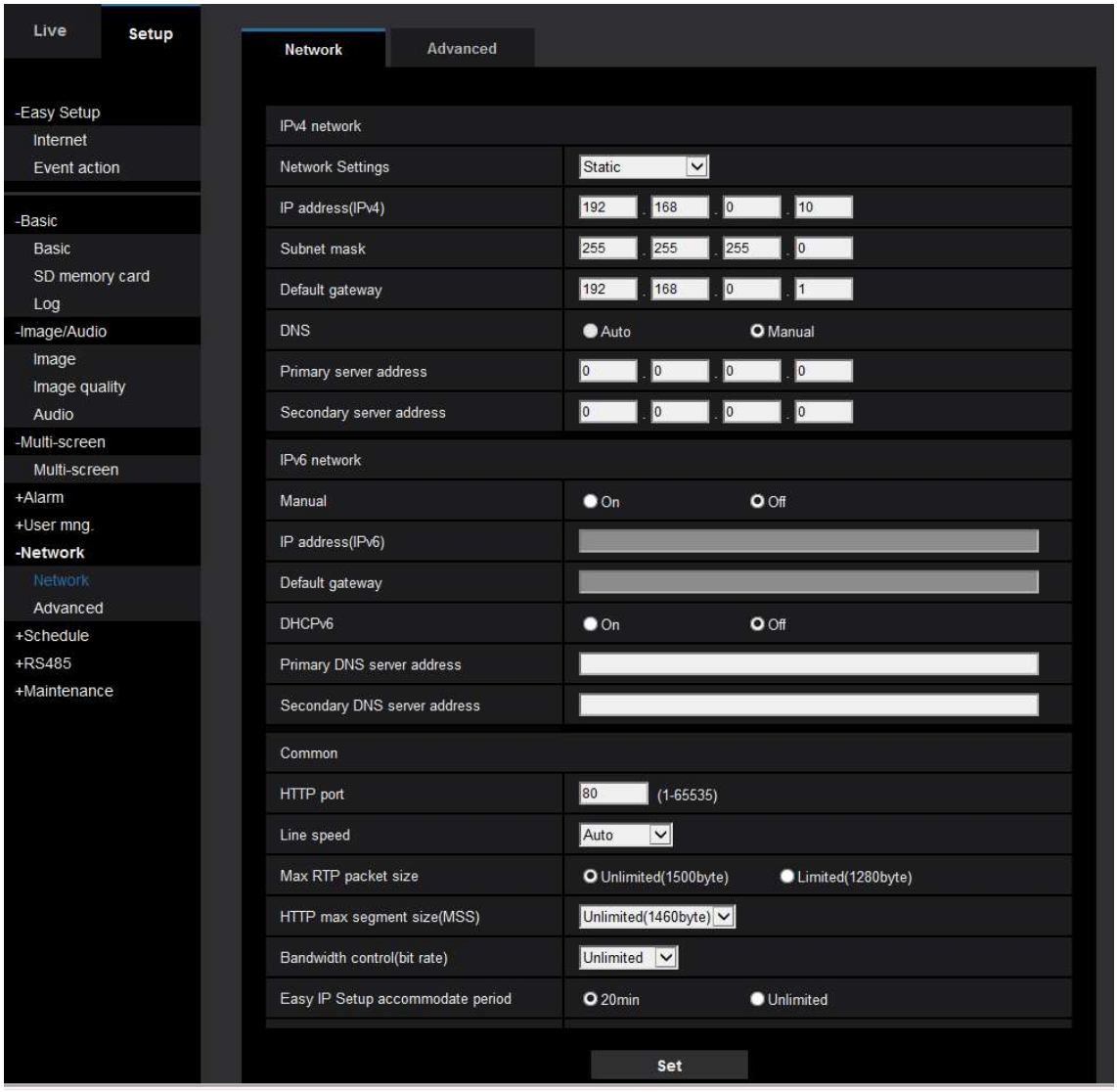
4.4. RTSP

RTSP used for streaming, like HTTP, does not handle communications encrypted by SSL. There is thus a risk of ID and password being snooped on. To prevent that, communications by HTTPS can be used or encrypted communications is possible by streaming in Internet mode as described below. Internet mode setting can be configured by turning on Internet mode (over HTTP) in the setting items for each stream from Image/Audio settings.



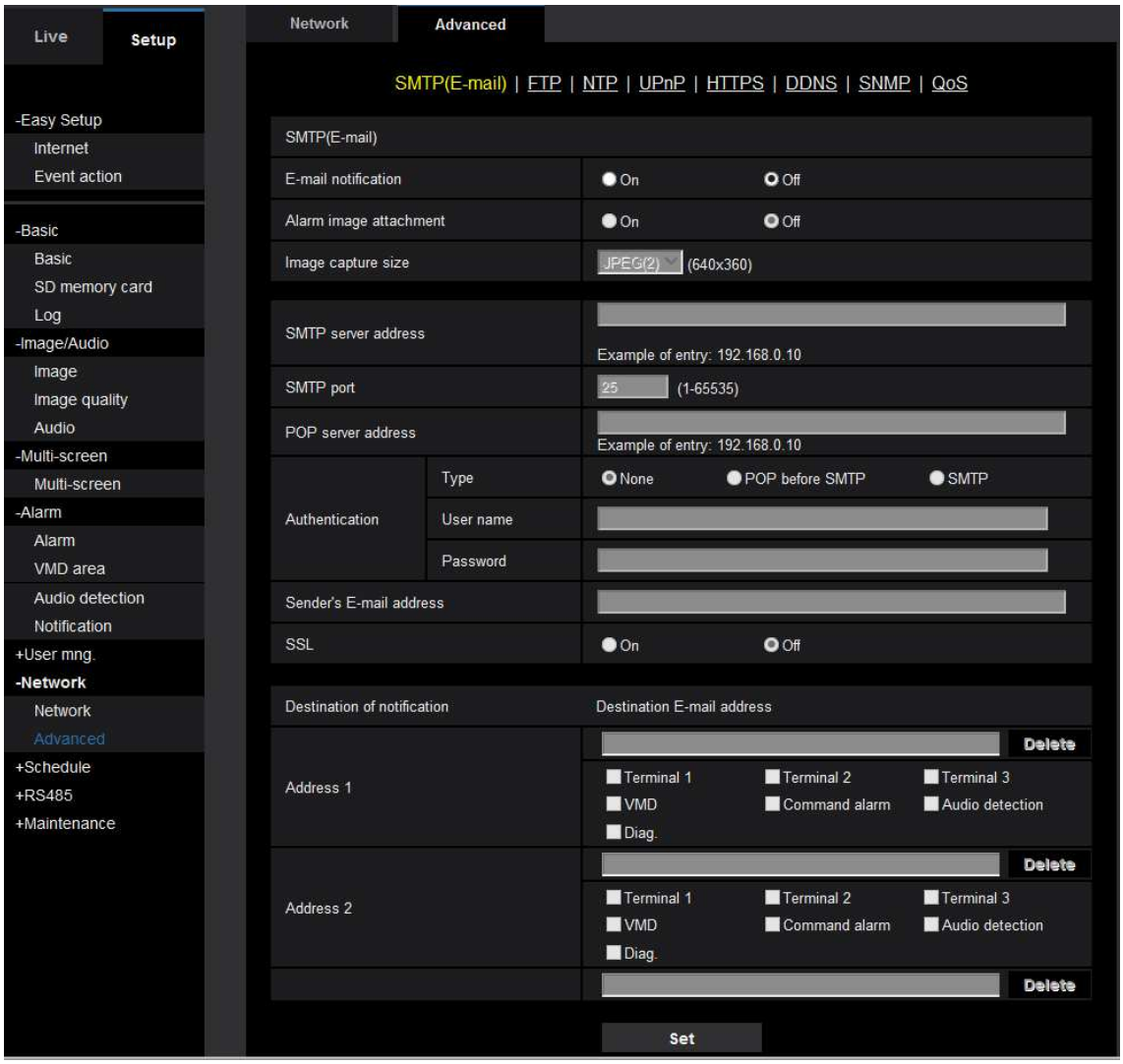
4.5. Easy IP

By activating the camera's easy IP setting cameras on the same network can be searched from the Easy IP Setup tool. Third parties will be able to make unauthorized access by obtaining the camera's IP address, and the risk of unauthorized infiltration and DoS attacks increases. In order to make so cameras cannot be searched from the Easy IP Setup tool when camera easy setup is completed, it is recommended that you limit the accommodate period of Easy IP Setup from Unlimited to 20 minutes. Easy IP Setup can be limited by setting Easy IP Setup accommodate period to 20min from the Network screen.



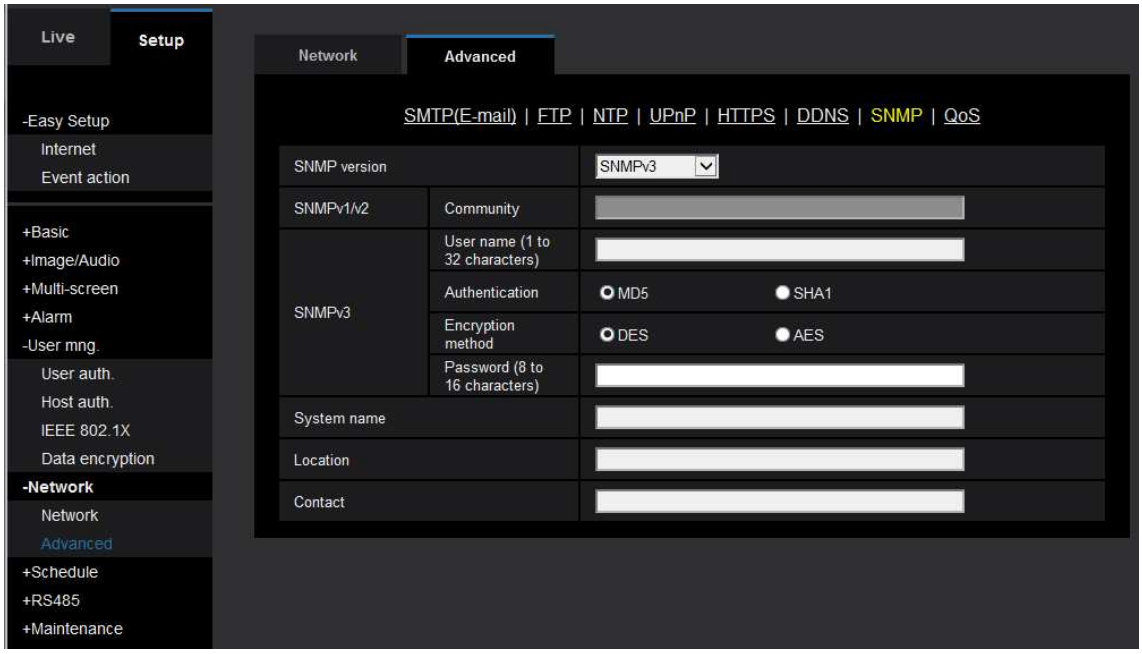
4.6. SMTP

When sending email by SMTP, the ID and password are not encrypted when connecting to the SMTP severer, so there is a risk of them being snooped on. Therefore, sending email to a server that supports SMTP over SSL is recommended when sending mail by SMTP. SMTP over SSL can be activated by turning SSL on at the SMTP(E-mail) settings screen.



4.7. SNMP

With SNMP v1/v2, packets themselves are not encrypted, so packets can be snooped on or altered. When using in an environment where there is risk of snooping or altering by a third party, use of SNMPv3 with encryption and altering detection functions is recommended. SNMPv3 can be used by setting SNMP Version to v3 from the SNMP settings screen.



5. Conclusion

There are potentially many threats to video surveillance systems, such as snooping, alteration of data, and spoofing of devices. So resistance to those threats will probably become even more important in the future with advances in IoT. Panasonic is continuously working to improve security to achieve a safe and secure society from the perspective of cyber security by quickly identifying and overcoming those threats.