

# SHARP®

インフォメーションディスプレイ

形名

**PN-ME652**

**PN-ME552**

**PN-ME502**

**PN-ME432**

セキュア通信によるコマンド制御について

# セキュア通信で本機を制御する(LAN)

本機をネットワークに接続し、ネットワーク上のコンピューターから安全な暗号化通信を使用して本機を制御することができます。

## ご参考

- 本機をネットワークに接続する必要があります。
- 設定メニューの「管理者設定」→「ネットワーク」の「イーサネット」をオンにし、ネットワークの設定をします。
- 設定メニューの「管理者設定」→「ネットワーク」の「モニター制御」の「ネットワークディスプレイ制御」をオンにします。
- 設定メニューの「管理者設定」→「本体設定」の「アドバンス」の「外部制御端子」を「LAN」にし、他の設定も行います。

```
C:\ssh-key>ssh-keygen.exe -t rsa -m RFC4716 -b 2048 -N "user1" -C "rsa_2048_user1" -f id_rsa
Generating public/private rsa key pair.
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:NB7PiZnl+S10sig5P0lne+h7AarPOP0z9BUpHl
20SzU rsa_2048_user1
The key's randomart image is:
+----[RSA 2048]-----+
|
|                Eo|
|   xxxxxxxxxxxxxxx|
|                .*=+*=|
+----[SHA256]-----+
```

4. id\_rsa(秘密鍵)とid\_rsa.pub(公開鍵)が作成されます。秘密鍵は大事に保管してください。コマンドの詳細は各ツールの説明を参照してください。

## セキュア通信による制御

公開鍵暗号方式によるユーザー認証と暗号化通信を行うことができます。セキュア通信を行うには、事前に秘密鍵と公開鍵を作成し、公開鍵を本機に登録する必要があります。またセキュア通信に対応したクライアントソフトウェアも必要になります。本機の制御には、Nフォーマットコマンド、及びSフォーマットコマンドを使用します。各フォーマットの説明書も合わせてお読みください。

## 秘密鍵・公開鍵の作成

OpenSSLやOpenSSH、一般のターミナルソフトウェアを使用して秘密鍵と公開鍵を作成します。

本機では下記の公開鍵方式をサポートします。

RSA(2048~4096bit)
DSA
ECDSA-256
ECDSA-384
ECDSA-521
ED25519

Windows10(バージョン1803以降)、Windows11では標準でOpenSSHを利用できます。OpenSSH(ssh-keygen)を使用したRSA鍵の作成の手順を説明します。

1. スタートボタンからコマンドプロンプトを起動します。
2. 鍵を作成するには次のコマンドを送ります。
3. 鍵の設定:

key type:	RSA
length:	2048bit
passphrase:	user1
public key comment:	rsa_2048_user1
file name:	id_rsa

## 公開鍵の登録

本機に設定メニューから公開鍵を登録します。

1. 公開鍵ファイル(上記例ではid\_rsa.pub)をUSBメモリにコピーします。
2. USBメモリを本機のUSB1端子に接続します。
3. 設定メニューの「管理者設定」→「ネットワーク」の「モニター制御」の「認証にセキュアなプロトコルを使用」をオンにします。
4. 「公開鍵ファイル」の「アップロード」を選択すると、ファイル選択画面が表示されます。
5. USBメモリ上の公開鍵ファイルを選択すると公開鍵が登録されます。登録した公開鍵ファイルは、ダウンロード、削除が可能になります。

---

## セキュア接続によるコマンド制御

SSHの認証機能・暗号化機能を使用したセキュア通信で本機を制御することができます。事前に秘密鍵・公開鍵の作成、公開鍵の登録を行ってください。

### 1. 本機と接続する

- ① SSHクライアントを起動し、IP アドレス、データポート番号（初期値：10022）を指定して、SSHプロトコルで本機と接続します。
- ② ユーザー名（初期値：Admin）と登録した公開鍵用の秘密鍵(id\_rsa)を指定し、鍵作成時に指定した秘密鍵のパスフレーズを入力します。
- ③ 認証に成功すると接続されます。

### 2. 制御コマンドを送信して、本機を制御します。

- ① NフォーマットもしくはSフォーマットのコマンドを使用します。コマンドの詳細は各フォーマットの説明書を参照してください。

### ご参考

- コマンド通信のない時間が自動ログアウト時間（初期値：5分）を経過すると、切断されます。
- 通常接続とセキュア接続は同時に使用できません。