はじめに

Cisco Catalyst IR1101 高耐久性シリーズルータは、ベースモジュールを備えた次世代のモジュール型産業用ルータで、プラガブルモジュールを追加できます。プラガブルモジュールは、IR1101 プラットフォームに様々なインターフェイスを追加できる柔軟性を実現します。

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

IR1101 には、デュアル LTE プラガブル、mSATA SSD FRU、SFP、追加のイーサネットおよび非同期ポート、デジタル GPIO 接続などの重要な機能を追加する拡張モジュールも 2 つ用意されています。

IR1101 は、Cisco IOS XE オペレーティング システムを実行する初の IoT プラットフォームです。IOS-XE は Linux ベースの OS で、多数の機能が強化され、従来の IOS バージョンと比較して多くの機能を備えています。

ガイドのこの項には、次の内容も含まれています。

IR1101 ベースルータ

次の図は、IR1101 の前面パネルを示し、その一部の機能を強調表示しています。

図 *1 : IR1101* の前面パネル

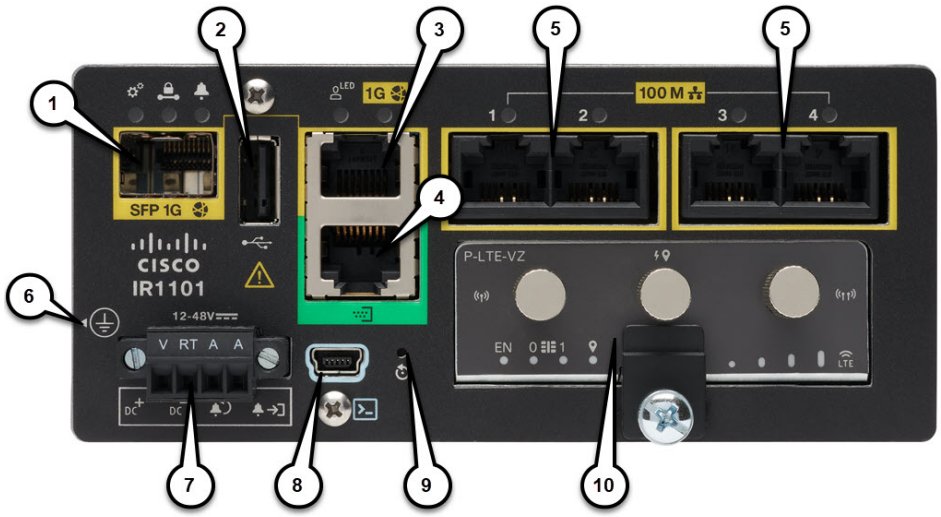


表 *1 :* 前面パネルの説明

アイテム	説明
1	SFP GigE WAN ポート（次の #3 のコンボ ポート）
2	タイプ A USB 2.0 ホスト ポート
3	RJ45 GigE WAN ポート（上記 #1 のコンボ ポート）
4	非同期シリアル ポート（DTE のみ）
5	RJ45 ファスト イーサネット LAN ポート
6	接地点 （デバイスの側面）
7	DC 電源およびアラーム入力
8	タイプ B ミニ USB コンソール ポート
9	リセット ボタン
10	プラガブル モジュール スロット（例：4G/LTE モジュール）

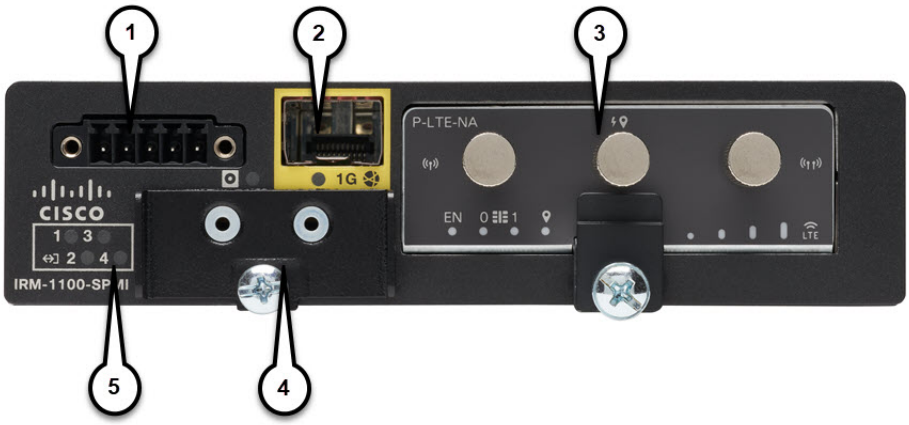
IRM-1100 拡張モジュール

拡張モジュールには、次の 2 つのタイプがあります。

- IRM-1100-SPMI
- IRM-1100-SP

次の図は、IRM-1100-SPMI の前面パネルを示し、その機能の一部を強調表示しています。

図 *2 : IR-1100-SPMI* 拡張モジュールの詳細



アイテム	説明
1	4 GPIO + 1 リターン（デジタル I/O） （注）　機能は Cisco IOS-XE リリース 16.12.1 以降で使用できます。
2	SFP コネクタ
3	プラガブルモジュール
4	mSATA SSD スロット
5	デジタル I/O LED

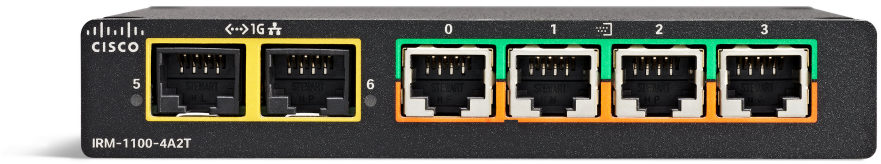
IR-1100-SP 拡張モジュールは、デジタル I/O および mSATA コンポーネントを持たない点以外は、IR-1100-SPMI モジュールと同じです。

詳細については、IRM-1101 拡張モジュールを参照してください。

IR1101 の詳細については、製品データシートを参照してください。

IRM-1100-4A2T 拡張モジュール

IRM-1100-4A2T は、IR1101 に取り付けることのできる拡張モジュールです。IR1101 への追加の 4 つの非同期シリアルポートと 2 つのイーサネット インターフェイスを提供します。次の図は、IRM-1100-4A2T を示しています。



IRM-1100-4A2T イーサネット インターフェイスは、レイヤ 2 RJ45 10/100/1000 Mbps ポートです。

IRM-1100-4A2T シリアルポートは、RJ45 コンボポート（RS232/RS485/RS422）です。

IR1101 には、拡張モジュールを取り付けられる側面が 2 つあります。上部は拡張側、下部はコンピューティング側と呼ばれます。追加モジュールが上部に接続されている場合は、拡張モジュール（EM）側として参照されます。追加モジュールが下部に接続されている場合は、コンピューティング モジュール（CM）側として参照されます。機能は、拡張モジュールがどちら側に取り付けられているか、および使用されている拡張モジュールの数と種類によって異なります。

IRM-1100-4A2T は、次のツールから管理できます。

- Cisco DNA Center
- WebUI

詳細については、IRM-1100-4A2T 拡張モジュールを参照してください。

- ルータ コンソールを使用して CLI にアクセスする方法 （4 ページ）
- リモート コンソールから CLI にアクセスする方法 （7 ページ）
- CLI セッション管理 （9 ページ）

ルータ コンソールを使用して CLI にアクセスする方法

Cisco IR1101 ルータには、USB のみに対応しているコンソール ポートがあります。コンソール ケーブル（Cisco P/N CAB-CONSOLE-USB、 長さ 6 フィート）は含まれていないため、注文する必要があります。

コンソール ポートは、シャーシの前面パネルにある USB 2.0 ミニ USB タイプ B コネクタです。デフォルトのボー レートは 9600 です。

ルータと通信する適切なドライバがないという警告がラップトップやPCに表示された場合は、ドライバをコンピュータ メーカーから入手するか、または次の URL を参照してください。
https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

工場出荷時のデバイスでは、システム設定ダイアログが表示されるため、基本的な設定の質問に回答してください。Cisco PnP 接続サービスを使用するためにルータを注文した場合、中央集中型プロビジョニングでは、ルータは最初のダイアログをスキップします。次に、例を示します。

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: <your-host-name>

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: <your-password>

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: <your-password>

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: <your-password>
Setup account for accessing HTTP server? [yes]: <return>
    Username  [admin]: <your-username>
    Password  [cisco]: <your-password>
    Password is UNENCRYPTED.
  Configure SNMP Network Management? [no]: <return>

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      NO  unset  up                    up
FastEthernet0/0/1      unassigned      YES unset  down                  down
FastEthernet0/0/2      unassigned      YES unset  down                  down
FastEthernet0/0/3      unassigned      YES unset  down                  down
FastEthernet0/0/4      unassigned      YES unset  up                    up
Async0/2/0             unassigned      YES unset  up                    down
Vlan1                  unassigned      YES unset  up                    up
```

（注） この次のセクションの名前と IP アドレスは例として示されています。

```
Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
  Configure IP on this interface? [no]: yes
    IP address for this interface: 192.168.1.1
    Subnet mask for this interface [255.255.255.0] : <return>
    Class C network is 192.168.1.0, 24 subnet bits; mask is /24

Would you like to configure DHCP? [yes/no]: yes
 Enter DHCP pool name: wDHCPool
 Enter DHCP network: 192.168.1.0
 Enter DHCP netmask: 255.255.255.0
 Enter Default router: 192.168.1.1

The following configuration command script was created:

hostname <your-hostname>
enable secret 9 $9$Z6fl74fvoEdMgU$XZYs8l4phbqpXsb48l9bzCng3u4Bc2kh1STsoLoHNes
enable password <your-enable-password>
line vty 0 4
password <your-password>
username <your-username> privilege 15 password <your-password>
no snmp-server
!
!
interface GigabitEthernet0/0/0
shutdown
no ip address
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface FastEthernet0/0/4
!
interface Vlan1
no shutdown
ip address 192.168.1.1 255.255.255.0
no mop enabled
ip dhcp pool wDHCPool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...

[OK]
```

```
Use the enabled mode 'configure' command to modify this configuration.


Press RETURN to get started! <return>


*Jul 27 21:35:24.369: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-3211716068
 has been generated or imported by crypto-engine
*Jul 27 21:35:24.372: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jul 27 21:35:24.448: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write
 memory" to save new IOS PKI configuration
*Jul 27 21:35:24.532: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named
TP-self-signed-3211716068.server has been generated or imported by crypto-engine
hostname>
```

これでデバイスに構築可能な基本設定ができました。

コンソール インターフェイスの使用方法

ステップ 1 次のコマンドを入力します。

```
Router > enable
```

ステップ 2 （イネーブル パスワードが設定されていない場合は、ステップ 3 に進みます）パスワード プロンプトで、システム パスワードを入力します。

```
Password: enablepass
```

パスワードが許可されると、特権 EXEC モード プロンプトが表示されます。

```
Router#
```

これで、特権 EXEC モードの CLI へのアクセスが可能になりました。必要なコマンドを入力して、必要なタスクを実行できます。

ステップ 3 コンソール セッションを終了するには、**quit** コマンドを入力します。

```
Router# quit
```

リモート コンソールから CLI にアクセスする方法

IR1101 のリモート コンソールには、Telnet またはよりセキュアな SSH を使用してアクセスできます。telnet アクセスの詳細については、この章の以降の項を参照してください。SSH アクセスの詳細については、「セキュア シェルの設定」を参照してください。

ここでは、リモート コンソールから CLI にアクセスする手順について説明します。

Telnet を使用してルータ コンソールに接続するための準備

詳細については、https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.htmlの Cisco IOS-XE デバイス強化ガイドを参照してください。

診断バナーおよび待機バナーの設定は任意ですが、設定することを推奨します。バナーは、特に Telnet または SSH 試行ステータスをユーザに示すインジケータとして役立ちます。

TCP/IP ネットワークから Telnet を使用してルータにリモート アクセスするには、**line vty** グローバル コンフィギュレーション コマンドを使用して、仮想端末回線をサポートするようにルータを設定します。ユーザに対してログインとパスワードの指定を要求するように、仮想端末回線を設定します。

line vty グローバル コンフィギュレーション コマンドの詳細については、『Cisco IOS Terminal Services Command Reference』ドキュメントを参照してください。

回線上でログインが無効化されないようにするには、**login** コマンドの設定時に **password** コマンドを使ってパスワードを指定します。

認証、認可、アカウンティング（AAA）を使用する場合は、**login authentication** コマンドを設定します。login authentication コマンドを使用してリストを設定するときに、回線上で AAA 認証に関するログインが無効化されないようにするには、**aaa authentication login** グローバル コンフィギュレーション コマンドを使用して、リストを設定する必要もあります。

AAA サービスの詳細については、『Cisco IOS XE Security Configuration Guide: Secure Connectivity』および『Cisco IOS Security Command Reference』を参照してください。**login line-configuration** コマンドの詳細については、『Cisco IOS Terminal Services Command Reference』を参照してください。

また、ルータに Telnet 接続する前に、ルータの有効なホスト名、またはルータに設定された IP アドレスを取得しておく必要もあります。Telnet を使用してルータに接続するための要件の詳細、Telnet サービスのカスタマイズ方法、および Telnet キー シーケンスの使用方法については、『Cisco IOS Configuration Fundamentals Configuration Guide』を参照してください。

Telnet を使用してコンソール インターフェイスにアクセスする方法

ステップ 1 端末または PC から次のいずれかのコマンドを入力します。

- **connect host** *[port] [keyword]*
- **telnet host** *[port] [keyword]*

ここで、*host* にはルータのホスト名または IP アドレスを指定し、*port* には 10 進数のポート番号（デフォルトは 23）を指定します。また、*keyword* にはサポートされるキーワードを指定します。これらのコマンドの詳細については、『Cisco IOS Terminal Services Command Reference』を参照してください。

（注） アクセスサーバを使用する場合は、ホスト名または IP アドレスに加えて、有効なポート番号（たとえば **telnet 172.20.52.40 2004**）を指定します。

次に、**telnet** コマンドを使用して、**router** という名前のルータに接続する例を示します。

```
unix_host% telnet router
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
unix_host% connect
```

ステップ 2 ログイン パスワードを入力します。

```
User Access Verification
Password: mypassword
```

（注） パスワードが設定されていない場合は、Return を押します。

ステップ 3 ユーザ EXEC モードから、**enable** コマンドを入力します。

```
Router> enable
```

ステップ 4 パスワード プロンプトで、システム パスワードを入力します。

```
Password: enablepass
```

ステップ 5 **イネーブル** パスワードが許可されると、特権 EXEC モード プロンプトが次のように表示されます。

```
Router#
```

ステップ 6 これで、特権 EXEC モードの CLI へのアクセスが可能になりました。必要なコマンドを入力して、必要なタスクを実行できます。

ステップ 7 Telnet セッションを終了するには、**exit** または **logout** コマンドを使用します。

```
Router# logout
```

CLI セッション管理

非アクティブ タイムアウトを設定して、強制的に適用することができます。セッション ロックにより、2 人のユーザが別々に行った変更を相互に上書きできないように保護できます。使用可能なすべてのキャパシティが内部プロセスによって使用されるのを防ぐために、CLI セッション アクセス用に予備の容量が予約されています。たとえば、これによりユーザはルータにリモート アクセスすることができます。

CLI セッション管理について

非アクティブ タイムアウトを設定して、強制的に適用することができます。セッション ロックにより、2 人のユーザがそれぞれ行った変更を相互に上書きできないように保護できます。使用可能なすべてのキャパシティが内部プロセスによって使用されるのを防ぐために、CLI セッション アクセス用に予備の容量が予約されています。たとえば、これによりユーザはルータにリモート アクセスできます。

CLI セッション タイムアウトの変更

ステップ 1 **configure terminal**

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **line console 0**

ステップ 3 **session-timeout** *minutes*

minutes の値により、タイムアウトになるまでの CLI の待機時間が設定されます。CLI セッション タイムアウトを設定すると、CLI セッションのセキュリティが強化されます。*minutes* に値 0 を指定すると、セッション タイムアウトが無効になります。

ステップ 4 **show line console 0**

セッション タイムアウトとして設定された値を確認します（"Idle Session" の値として表示されます）。

CLI セッションのロック

始める前に

CLI セッションの一時パスワードを設定するには、EXEC モードで **lock** コマンドを使用します。**lock** コマンドを使用するには、その前に **lockable** コマンドを使用して回線を設定する必要があります。次の例では、回線が **lockable** として設定され、その後 **lock** コマンドを使用して一時パスワードが割り当てられます。

ステップ 1 **Router# configure terminal**

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **lock** コマンドを使用できるようにする回線を入力します。

```
Router(config)# line console 0
```

ステップ 3 **Router(config)# lockable**

回線をロック可能にします。

ステップ 4 **Router(config)# exit**

ステップ 5 **Router# lock**

パスワードの入力が求められます。パスワードを 2 回入力する必要があります。

```
Password: <password>
Again: <password>
Locked
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。