



Cisco IOS-XE 17.2.1 の新機能

- [ネイティブ Docker のサポート \(1 ページ\)](#)
- [raw ソケットトランスポートに対する YANG データモデルのサポート \(2 ページ\)](#)
- [IOx コンテナアプリケーションのデジタル IO \(3 ページ\)](#)
- [L2 スティックセキュア MAC アドレス \(4 ページ\)](#)
- [署名付きアプリケーションのサポート \(6 ページ\)](#)

ネイティブ Docker のサポート

ネイティブ Docker のサポートが 17.2.1 リリースに追加されました。この機能により、ユーザは Docker アプリケーションを IR1101 に展開できます。アプリケーションのライフサイクルプロセスは、「アプリケーションのインストールとアンインストール」の項の手順と同様です。Docker アプリケーションの場合、アプリケーション設定の一部としてエントリポイント設定が必要です。エントリポイントの設定については、次の例を参照してください。

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#app-hosting appid app3
Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.0.7 netmask 255.255.255.0
Router(config-app-hosting-gateway0)#app-default-gateway 192.168.0.1 guest-interface 0
Router(config-app-hosting)#app-resource docker
Router(config-app-hosting-docker)#run-opts 1 "--entrypoint '/bin/sleep 1000'"
Router(config-app-hosting-docker)#end
Router#
```

Docker アプリケーションの出力を次の例に示します。

```
Router#show app-hosting detail
App id : appl
Owner : iox
State : RUNNING
Application
Type : docker
Name : aarch64/busybox
Version : latest
Description :
Path : bootflash:busybox.tar
Activated profile name : custom
```

```

Resource reservation
Memory : 431 MB
Disk : 10 MB
CPU : 577 units
VCPU : 1
Attached devices
Type Name Alias
-----
serial/shell iox_console_shell serial0
serial/aux iox_console_aux serial1
serial/syslog iox_syslog serial2
serial/trace iox_trace serial3
Network interfaces
-----
eth0:
MAC address : 52:54:dd:e9:ab:7a
IPv4 address : 192.168.0.7
Network name : VPG0
Docker
-----
Run-time information
Command :
Entry-point : /bin/sleep 10000
Run options in use : --entrypoint '/bin/sleep 10000'
Application health information
Status : 0
Last probe error :
Last probe output :
Router#

```

raw ソケットトランスポートに対する YANG データモデルのサポート

リリース 17.2.1 では、追加の YANG データモデルに対するサポートが追加されています。これらの追加モデルには、raw ソケットトランスポートが含まれています。

YANG データモデルは次の URL で確認できます。

<https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1721>

メインの Cisco-IOS-XE ネイティブモデルに属する raw ソケットには 2 つの機能モジュールがあります。その内容は次のとおりです。

- Cisco-IOS-XE-rawsocket.yang

このモジュールには raw ソケットトランスポートのコンフィギュレーションコマンドの YANG 定義のコレクションが含まれています。

次に、このモジュールに対応する CLI コマンドを示します。

```

# encapsulation raw-tcp
# encapsulation raw-udp
# raw-socket packet-length <length>
# raw-socket packet-timer <timer>
# raw-socket special-char <value>
# raw-socket tcp server <port> <ip>

```

```
# raw-socket tcp idle-timeout <value>
# raw-socket tcp client <dest-ip> <dest-port>
# raw-socket tcp idle-timeout <timeout>
# raw-socket tcp tcp-session <value>
# raw-socket tcp dscp <value>
# raw-socket udp connection <dest-ip> <dest-port> <local_port>
```

- Cisco-IOS-XE-rawsocket-oper.yang

このモジュールには、raw ソケットトランスポートの運用データの YANG 定義のコレクションが含まれています。

次に、このモジュールに対応する CLI コマンドを示します。

```
# show raw udp statistics
# show raw tcp statistics
# show raw tcp session
# show raw udp session
# show raw tcp session local
# show raw udp session local
```

次に、依存モジュールのリストを示します。

- Cisco-IOS-XE-native
- Cisco-IOS-XE-features
- ietf-inet-types
- Cisco-IOS-XE-interfaces
- Cisco-IOS-XE-ip
- Cisco-IOS-XE-vlan
- ietf-yang-types @ (すべてのリビジョン)
- cisco-semver

IOx コンテナアプリケーションのデジタル IO

リリース 17.2.1 では、IOx コンテナアプリケーションがデジタル IO にアクセスできるようになりました。alarm contact コマンドに新しい CLI が追加されました。

```
Router(config)# alarm contact ?
  <0-4>           Alarm contact number (0: Alarm port, 1-4: Digital I/O)
  attach-to-iox  Enable Digital IO Ports access from IOX
Router (config)# alarm contact attach-to-iox
```

attach-to-iox コマンドを有効にすると、IOx へのすべてのデジタル IO ポートを完全に制御できます。ポートは、4 文字のデバイス /dev/dio-[1-4] として IOX アプリケーションに公開されます。読み取りまたは書き込みの機能を使用して、デジタル IO ポートの値を取得または設定できます。

モードを更新する場合は、モード値を文字型デバイスファイルに書き込むことができます。これは、状態の読み取り/書き込み、モードの変更、およびポートの真のアナログ電圧の読み取りを行う IOCTL コールによって実行されます。この方法に従って、アナログセンサーを IR1101 に接続できます。すべてのポートが最初に入力モードに設定され、電圧は 3.3v にプルアップされます。

次に、IOCTL コールの例を示します。

デジタル IO ポートの読み取り

```
cat /dev/dio-1
```

デジタル IO ポートへの書き込み

```
echo 0 > /dev/dio-1
echo 1 > /dev/dio-1
```

モード変更

```
echo out > /dev/dio-1
echo in > /dev/dio-1
```

サポートされている IOCTL のリスト

```
DIO_GET_STATE = 0x1001
DIO_SET_STATE = 0x1002
DIO_GET_MODE = 0x1003
DIO_SET_MODE_OUTPUT = 0x1004
DIO_SET_MODE_INPUT = 0x1005
DIO_GET_THRESHOLD = 0x1006
DIO_SET_THRESHOLD = 0x1007
DIO_GET_VOLTAGE = 0x1009
```

IOCTL を使用した状態の読み取り

```
import fcntl, array
file = open("/dev/dio-1", "rw")
state = array.array('L', [0])
fcntl.ioctl(file, DIO_GET_STATE, state)
print(state[0])
```

IOCTL を使用したモードの変更

```
import fcntl
file = open("/dev/dio-1", "rw")
fcntl.ioctl(file, DIO_SET_MODE_OUTPUT, 0)
```

L2 スティックセキュア MAC アドレス

これは IR1101 には新機能ですが、IOS-XE にはしばらく前から搭載されていました。

スティッキーラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキーセキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。インターフェイスはスティッキーラーニングがイネーブルになる前に

学習したものを含め、すべてのダイナミックセキュア MAC アドレスをスティッキーセキュア MAC アドレスに変換します。すべてのスティッキーセキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキーセキュア MAC アドレスは、コンフィギュレーションファイル（スイッチが再起動されるたびに使用されるスタートアップコンフィギュレーション）に、自動的に反映されません。スティッキーセキュア MAC アドレスをコンフィギュレーションファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキーセキュア アドレスを保存しない場合、アドレスは失われます。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレステーブルに追加されている状態で、アドレステーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。

違反が発生した場合の対処に基づいて、次の3種類の違反モードのいずれかにインターフェイスを設定できます。

- **protect**（保護）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないうえ、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。

Note：スティッキラーニングが無効になっている場合は、スティッキーセキュア MAC アドレスがダイナミックセキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

- **restrict**（制限）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないうえ、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
- **shutdown**（シャットダウン）：ポートセキュリティ違反により、インターフェイスが **error-disabled** になり、ただちにシャットダウンされます。そのあと、ポートの LED が消灯します。セキュア ポートが **error-disabled** ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこのステートを解除するか、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して手動で再び有効にできます。これは、デフォルトのモードです。
- **shutdown vlan**（VLAN シャットダウン）：VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が **errdisable** になります。

コマンドラインインターフェイス

スイッチインターフェイスに `port-security cli` を追加します。

```
Router(config-if)#switchport port-security ?  
  aging          Port-security aging commands  
  mac-address    Secure mac address  
  maximum        Max secure addresses  
  violation      Security violation mode  
  <cr>          <cr>  
Router(config-if)#switchport port-security mac-address sticky
```

署名付きアプリケーションのサポート

シスコの署名付きアプリケーションが IR1101 でサポートされるようになりました。署名付きアプリケーションをインストールするには、デバイスで署名付き検証を有効にする必要があります。署名付き検証を有効にするには、次の手順を実行します。

```
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#  
Router(config)#app-hosting signed-verification  
Router(config)#  
Router(config)#exit
```

署名付き検証を有効にした後、「IOx アプリケーションホスティング」の「アプリケーションのインストールとアンインストール」の項の手順に従ってアプリケーションをインストールします。

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。