6 リモート管理

概　要

最新のソフトウェア・リリースを使用すると、本装置をリモートで管理することができます。リモート管理機能は、次のプロトコルに対応しています。

- Telnet
- Secure Shell(SSH)
- SNMP

リモート管理機能を有効にして、その設定を行うには、ローカルのシリアル・コンソールが必要です。

リモート管理機能を有効にすると、遠隔地のマシンで実行中のTelnetセッションまたはSSHセッションから、デバイスのコマンドライン・インターフェース(CLI)にアクセスすることができます。リモート・セッションは、Telnetセッションおよび SSHセッションを含めて、最大5つ設定することができます(デフォルトは5)。デバイスのリモート管理機能を使用するには、ローカルのシリアル・コンソールでリモート管理を有効にして、その設定を行う必要があります。リモート管理機能を使用するには、デバイスのネットワーク・インターフェースにIPアドレスを割り振る必要があります。
SNMPのリモート管理機能については、MIB-IIのシステム・グループ管理まで、サポートされています

制限事項

ローカル・コンソールで使用可能なCLI機能のいくつかは、リモート・セッションでは使用できないことに注意してください。以下にそれらを示します。

- 本装置のネットワーク・インターフェースに対するIPアドレスの割り当て
- Telnet、SSH、またはSNMPの有効/無効の切り替え
- Telnet、SSH、またはSNMPのポートの変更
- Telnetセッション、またはSSHセッションの数の変更
- 監視レポート機能またはアラーム機能の有効/無効の切り替え(ただし、リモート管理機能を有効にする前に、レポート機能およびアラーム機能をシリアル・コンソールで有効にしておけば、レポートおよびアラームをリモートで受け取ることができます)。

リモート管理用のCLIコマンドを使用すると、デバイスの設定ファイルに影響が及ぶことがあります。デバイスを再起動してもリモート管理の設定内容が失われないようにするためには、CLIコマンドのconfig saveを使って、リモート管理の設定を保存する必要があります。これにより、設定は起動時に復元されます。

リモート管理用CLIコマンド

リモート管理機能は、ローカルのシリアル・コンソールから一連のCLIコマンドを使用して、有効/無効を切り替えたり、設定を行ったりすることができます。正確なシーケンスは、有効にしたいリモート・セッションのタイプや設定によりさまざまです(使用方法については、この後のセクションで説明します)。これらのコマンドを以下に示します。

共通:

- set ip <ip> <netmask>は、本装置のネットワーク・インターフェースにIPアドレスおよびネットマスクを割り当てます。
- set max_remote_sessions <1-5>は、同時に実行できるTelnetセッションおよびSSHセッションの最大数を設定します。

Telnet用:

- set telnet enable¦disableは、Telnetセッションの有効/無効を切り替えます。
- show telnetは、Telnetの現在の状況が有効、無効のどちらであるのかを表示します。
- set telnet_port <port>は、Telnetのポートを設定します(デフォルトは23です)。
- show telnet_portは、Telnetの現在のポートを表示します。

SSH用:

- set ssh enable¦disableは、SSHセッションの有効/無効を切り替えます。
- show sshは、SSHの現在の状況が有効、無効のどちらであるのかを表示します。
- set ssh_port <port>は、SSHのポートを設定します(デフォルトは22です)。
- show ssh_portは、SSHの現在のポートを表示します。

SNMP用:

- setsnmp snmp enable¦disableは、SNMP管理機能の有効/無効を切り替えます。
- showsnmp snmpは、SNMPの現在の状況が有効、無効のどちらであるのかを表示します。
- setsnmp snmp_infoは、以下に示すSNMPの情報およびパラメータを設定します。
  - SNMP port (デフォルトは161)
  - SNMP trap port (デフォルトは162)
  - SNMP agent IP address
  - Contact person(管理者)
  - System name(システム名)
  - System location(設置場所)
- showsnmp snmp_infoは、SNMPの現在の情報およびパラメータを表示します。
- setsnmp snmp_communityは、SNMPコミュニティ文字列および管理コンソールのIPアドレスを設定します。
- list snmp_communityは、SNMPコミュニティ文字列および管理コンソールのIPアドレスを表示します。
- delete snmp_communityは、SNMPコミュニティ設定を削除します。
- setsnmp trap_communityは、SNMPトラップ送信時のコミュニティと送信先IPアドレスを設定します。
- list trap_communityは、SNMPトラップ送信時のコミュニティと送信先IPアドレスを表示します。
- delete trap_communityは、SNMPトラップ設定を削除します

リモートTelnetセッション

このセクションでは、リモートTelnetセッションを介して、本装置のCLIにアクセスする手順を説明します。

ローカル・シリアル・コンソール

以下の手順で、本装置のネットワーク・インターフェースにIPアドレスを割り当てます。

```
Intel 7110> set ip
Enter IP [10.1.2.56]: 10.1.1.1
Enter Netmask [255.255.255.0]:
```

IPおよびネットマスクを確認します(任意)。

```
Intel 7110> show ip
System IP Address : None
System Netmask    : None
Intel 7110>
```

リモートTelnetセッションを有効にします。

```
Intel 7110> set telnet enable
```

ネットワーク・ルートを設定します(管理用ネットワーク通信が用いるデフォルト・ルートを設定します)。

```
Intel 7110> set route
Enter Default Route ('none' to delete)
[10.1.1.1] : <enter>
```

ルート設定を確認します(任意)。

```
Intel 7110> show route
Default Route : 10.1.1.1
```

ルート設定を削除します(任意)。

```
Intel 7110> set route none
```

以上で本装置のリモートTelnet管理機能が設定され、使用できるようになります。これで、リモートTelnetセッションによって、CLIにアクセスすることができます。

デバイスを再起動しても、リモート管理の設定内容が失われないようにするには、config saveコマンドを実行します。

リモート・コンソール、Telnet

リモートTelnetを本装置上で有効にしたら、以下の手順で本装置のCLIにアクセスします。

```
Unix-prompt> telnet 10.1.1.1
Trying 10.1.1.1...
Connected to 10.1.1.1.
Escape character is '^]'.
.
.
.
Serial 0:a0:a5:11:4:2e
password:<password>
```

パスワードを入力すると、Telnetセッションは、本装置のCLIを表示します。これ以降、ローカルのシリアル・コンソールから行うのと同様に、デバイスを管理することができます(ただし、本章初めの「制限事項」に示したコマンドは使用できません)。

他のリモート・セッションがすでに実行されていて、新しいセッションを確立すると、セッション数がset max_remote_sessionsコマンドで設定した値を超えてしまう場合は、「Max Remote Sesion Limit of (5) exceeded!」というメッセージが表示されます。この場合は、セッションを終了するか、許可されるセッションの最大数を増やしてください。

Telnetポートの変更

Telnetポートを設定または表示するには、CLIコマンドのset telnet_port <port>またはshow telnet_portを使用します。
これらのコマンドを実行できるのは、ローカルのシリアル・コンソールからだけです。ただし、リモート管理機能を有効にしておく必要があります。デフォルトでは、Telnetポート番号は23です。

Telnet用ポートを設定するには、次のようにします。

```
Intel 7110> set telnet_port 230
```

使用しているTelnet用ポートを表示するには、次のようにします。

```
Intel 7110> show telnet_port
Telnet Port Number: 230
```

Telnetの無効

Telnetは、本装置のローカル・シリアル・コンソールから無効にすることができます。そのための手順を以下に示します。

```
Intel 7110> set telnet disable
```

Telnetが無効になったことを確認するには、次のようにします。

```
Intel 7110> show telnet
Telnet: disable
```

デバイスを再起動しても、Telnetセッションを無効のままにしたい場合は、config saveコマンドを実行します。

リモートSSHセッション

このセクションでは、リモートSSH(Secure Shell)セッションを介して、本装置のCLIにアクセスする手順を説明します。

ローカル・シリアル・コンソール

以下の手順で、本装置のネットワーク・インターフェースにIPアドレスを割り当てます。

```
Intel 7110> set ip
Enter IP [10.1.2.56]: 10.1.1.1
Enter Netmask [255.255.255.0]:
```

IPおよびネットマスクを確認します(任意)。

```
Intel 7110> show ip
System IP Address: 10.1.1.1
System Netmask: 255.255.255.0.
```

リモートSSHセッションを有効にします。

```
Intel 7110> set ssh enable
```

ネットワーク・ルートを設定します。

```
Intel 7110> set route
Enter Default Route ('none' to delete)
[10.1.1.1] : <enter>
```

ルート設定を確認します(任意)。

```
Intel 7110> show route
Default Route : 10.1.1.1
```

ルート設定を削除します(任意)。

```
Intel 7110> set route none
```

以上で本装置のリモートSSH管理機能が設定され、使用できるようになりました。これで、リモートSSHセッションから、CLIにアクセスすることができます。

デバイスを再起動しても、リモート管理の設定内容が失われないようにするには、config saveコマンドを実行します。

リモート・コンソール、SSH

リモートSSHを本装置上で有効にしたら、以下の手順で本装置のCLIにアクセスします。

```
Unix-prompt> ssh -1 admin 10.1.1.1
:
:
:
Serial 0:a0:a5:11:4:2e
password:<password>
```

パスワードを入力すると、SSHセッションは、本装置のCLIを表示します。これ以降、ローカルのシリアル・コンソールから行うのと同様に、デバイスを管理することができます(ただし、本章初めの「制限事項」に示したコマンドは使用できません)。

他のリモート・セッションがすでに実行されていて、新しいセッションを確立すると、セッション数がset max_remote_sessionsコマンドで設定した値を超えてしまう場合は、「Max Remote Sesion Limit of (5) exceeded!」というメッセージが表示されます。この場合は、セッションを終了するか、許可されるセッションの最大数を増やしてください。

SSH用ポートの変更

SSH用ポートを設定または表示するには、CLIコマンドのset ssh_port <port>またはshow ssh_portを使用します。
これらのコマンドを実行できるのは、ローカルのシリアル・コンソールからだけです。ただし、リモート管理機能を有効にしておく必要があります。デフォルトでは、SSHポート番号は22です。

SSH用ポートを設定するには、次のようにします。

```
Intel 7110> set ssh_port 220
```

使用しているSSH用ポートを表示するには、次のようにします。

```
Intel 7110> show ssh_port
SSH Port Number: 220
```

SSHを無効にする

SSHは、本装置のローカル・シリアル・コンソールから無効にすることができます。そのための手順を以下に示します。

```
Intel 7110> set ssh disable
```

SSHが無効になったことを確認するには、次のようにします。

```
Intel 7110> show ssh
SSH: disable
```

デバイスを再起動しても、SSHセッションを無効のままにしたい場合は、config saveコマンドを実行します。

SNMP

本装置は、業界標準に準拠した組み込み式のSNMPエージェントです。SNMPv1要求とSNMPv2要求をサポートしています。Intelプライベート・エンタープライズMIBは、標準MIB-IIの他にも、以下のような機能を提供しています。

- 本装置のハードウェアおよびネットワーク・リンクの障害の監視
- アラーム機能および監視機能の有効/無効を示すフラグの監視
- CPU使用率、同時オープンコネクション総数、1秒毎の処理コネクション数などで示される本装置の負荷の監視
- SSLの暗号化/復号化機能の状況およびパフォーマンスの監視
- 過負荷、スピル、スロットルの監視

業界標準への準拠

本装置のSNMPエージェントは、SNMPv1要求およびSNMPv2c要求という、2つの規格に対応しています。Intelプライベート・エンタープライズMIBファイルは、RFC1902に規定されているSMIv2に準拠しています。本装置では、どのIntelプライベートMIBオブジェクトに対しても、SET操作を行うことはできません。ただし、CLIからコマンドを使用すれば、MIB変数値を変更することができます。

Intel MIBツリー

図6-1は、Intel MIBツリーの最上位を示しています。

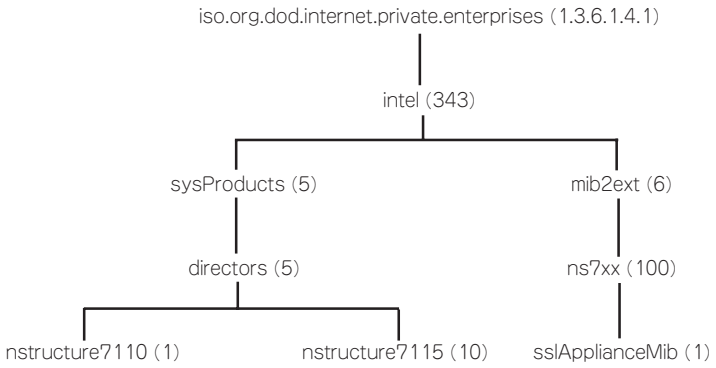

図6-1　Intel MIBツリー(最上位)

IntelエンタープライズMIBおよびMIBオブジェクトはすべて、Intelツリーのmib2extブランチの下で定義されます。Intel製品を識別するsysObjectIdsはすべて、Intelツリーのsysブランチの下で定義されます。

サポートされるMIB

管理情報ベースII(MIB-II)
以下のIntelエンタープライズMIB:

```
ceo-header.my
ssl-appliance-mib.my
```

MIBファイルの入手方法

MIBファイルの入手方法については、お問い合わせください。

SNMP SETを介しての書き込みアクセスは、どのMIB変数やSNMPグループに対しても行うことはできません。SNMP SETをグループに対して実行すると、エラーが戻されます。標準SNMPトラップとして、coldStart、warmStart、authenticationfailure、linkUp、およびlinkDownがサポートされています。

ceo-header.my

ceo-header.myには、Intel NetStructure製品に対して定義されたsysObjectIdsがすべて含まれています。sysObjectIdsはすべて、IntelツリーのsysProducts/directorsブランチの下で定義されます。このMIBファイルには、「7110 {343, 5, 5, 1}」というsysObjectIdが定義されています。

エンタープライズ・プライベートMIBの一覧

以下に、本装置のプライベートMIBの一覧を示します。

mode

```
inline(1): Device is configured to accelerate SSL traffic
bypass(2): Device is configured to pass through all SSL traffic
```

failMode

```
safe(1): Two ethernet segments fail open, stopping traffic
through(2): Two ethernet segments fail shorted, allowing traffic to
continue
```

spillMode

throttle(1): Device will throttle SSL connections when utilization reaches 100%

spill(2): Device will spill SSL connections when utilization reaches 100%

sslSessionCache

enabled(1): SSL session caching is turned on

disabled(2): SSL session caching is turned off

restarts

Number of times the system has restarted

appLastRestart

The value of sysUpTime at the time the last restart of the application process happened

encryptionAlarm

enabled(1): Encryption status change alarm is turned on

disabled(2): Encryption status change alarm is turned off

sslConnectionAlarm

enabled(1): SSL connection alarm is turned on

disabled(2): SSL connection alarm is turned off

thresholdAlarm

enabled(1): Threshold alarm is turned on

disabled(2): Threshold alarm is turned off

overloadAlarm

enabled(1): Overload alarm is turned on

disabled(2): overload alarm is turned off

linkStatusAlarm

enabled(1): Network link status alarm is turned on

disabled(2): Network link status alarm is turned off

encryptProcessingState

on(1): SSL processing on

off(2):SSL processing halted

encryptProcessingStateReason

normal(1): Normal

hardware(2): Change caused by hardware fault

consoleBypass(3): Bypass mode enabled at console

consoleInline(4): Inline mode enabled at console

frontPanelBypass(5): Bypass mode enabled at front panel

frontPanelInline(6): Inline mode enabled at front panel

serverInterfaceState

State of the server-side interface

networkInterfaceState

State of the network-side interface

utilWindow

Sliding window (in seconds) to calculate average connections, CPU utilization, and active connnection rates

cpuUtil

CPU utilization percentage (0-100)

cpuUtilNetwork

CPU utilization percentage processing network traffic (0-100)

cpuUtilProxy

CPU proxy utilization percentage (0-100)

cpuUtilHiWater

CPU utilization high water mark (2-100)

cpuUtilLoWater

CPU utilization low water msrk (1-99)

cpuUtilState

When CPU utilization exceeds the hi water mark, CPU utilization state is in alert and is not returned to normal until the lo water threshold is crossed

sslCps

SSL connections per second

sslCpsMaximum

Maximum SSL connection rate in connections per second since (re)start

sslCpsHiWater

SSL connections per second high water mark

sslCpsLoWater

SSL connections per second low water mark

sslCpsState

When SSL connections per second exceeds the hi water mark, sslCpsState is in alert and is not returned to normal until the lo water threshold is crossed

sslConnCnt

Current number of concurrent open SSL connections

sslConnCntMaximum

Maximum number of concurrent open SSL connections since (re)start

sslConnTotal

Total number of SSL connections processed

sslConnCntHiWater

Concurrent open SSL connection count high water mark

sslConnCntLoWater

Concurrent open SSL connection count low water mark

sslConnCntState

When concurrent open SSL connection count exceeds the hi water mark, sslConnCntState is in alert and is not returned to normal until the lo water threshold is crossed

encryptedBps

Encryption rate in bytes per second

encryptedBpsMaximum

Maximum encryption rate in bytes per second since (re)start

encryptedBytesTotalMb

Total number of megabytes of data encrypted

decryptedBps

Decryption rate in bytes per second

decryptedBpsMaximum

Maximum decryption rate in bytes per second since (re)start

decryptedBytesTotalMb

Total number of megabytes of data decrypted

sslOverloadInterval

The periodic interval (in seconds) used when counting the number of spilled or throttled SSL connections. If any SSLconnections were spilled or throttled in the lastsslOverloadInterval, a trap is generated. If sslOverloadInterval is 0, no trap is generated

throttlesPerSec

Number of throttles per second

throttlesPerSecMaximum

Maximum number of throttles per second since (re)start

throttlesTotal

Total number of throttles since (re)start throttles

Total number of throttles in the last sslOverloadInterval

spillsPerSec

Number of spills per second

spillsPerSecMaximum

Maximum number of spills per second since (re)start

spillsTotal

Total number of spills since (re)start

spills

Number of spills in the last sslOverloadInterval

refusedSslInterval

The periodic interval (in seconds) used when counting the number of refused SSL connections. If any SSL connections were refused in this time interval, a trap is generated.

cipherSuiteMismatch

Number of refused SSL connections in the last refusedSslInterval which are due to inability of the client and server to agree upon a cipher suite

clientCertAuthFail

Number of refused SSL connections in the last refusedSslInterval which are due to authentication failure of the client certificate

トラップの一覧

以下に本装置により生成されたトラップを一覧にして示します。各トラップの詳細については、前述したMIBの説明、またはMIBファイル内のドキュメント参照してください。トラップは、SNMPが生成します。

標準SNMPトラップ

coldStart

warmStart

authenticationFailure

linkUp

linkDown

ssl-appliance-mib.myのプライベート・トラップ

encryptionStopped

Alert issued whenever the device stops processing SSL traffic

encryptionResumed

Resumes processing traffic after having been stopped

serverInterfaceStateChanged

The server-side interface state changed

networkInterfaceStateChanged

The network-side interface state changed

cpuUtilAlert

The device has exceeded the CPU utilization high water threshold

cpuUtilNormal

CPU utilization back to normal levels

sslCpsAlert

The device has exceeded the SSL connections per second high water threshold

sslCpsNormal

The SSL connections per second processed by the device is back to normal levels

sslConnCntAlert

The device has exceeded the open SSL connection count high water threshold

sslConnCntNormal

The open SSL connection count of the device is back to normal levels

sslConnectionRefusedMismatch

SSL connections were refused in the past sslRefusedInterval due to cipher suite negotiation

failuresslConnectionRefusedAuthFail

SSL connections were refused in the past sslRefusedInterval due to authentication failure of the client certificate

sslOverloadSpills

SSL connections were spilled in the past sslOverloadInterval

sslOverloadThrottles

SSL connections were throttled in the past sslOverloadInterval

appRestartAlert

SSL processing application has restarted

SNMPを有効にする

SNMPの有効/無効を切り替えるには、CLIコマンドのsetsnmp snmp enable¦disableを使用します。動作状況を調べるには、showsnmp snmpコマンドを使用します。

例:

```
Intel 7110> setsnmp snmp enable

Intel 7110> showsnmp snmp
SNMP: enable

Intel 7110> setsnmp snmp disable

Intel 7110> showsnmp snmp
SNMP: disable
```

SNMP情報の指定

SNMPパラメータは、以下に示すように、setsnmp snmp_infoコマンドを使用して、一度に設定することができます。

```
Intel 7110> setsnmp snmp_info
SNMP port [161]: 161
SNMP trap port [162]: 162
Contact Person []: support
System Location []:
System Name []: 7110
```

SNMPパラメータの値は、以下のように、shownmp snmp_infoコマンドを使用して表示することができます。

```
Intel 7110> showsnmp snmp_info
SNMP port: 161
SNMP trap port: 162
Contact Person: support
System Name: 7110
System IP Address: x.x.x.x
System Netmask: y.y.y.y
Default Route: z.z.z.z
```

SNMP情報の各項目は、以下のコマンドを使用して、個別に設定することもできます。

- setsnmp snmp_portは、SNMP portを設定します
- setsnmp trap_portは、SNMP trap portを設定します
- setsnmp sys_contactは、Contact Personを設定します
- setsnmp sys_nameは、System Nameを設定します
- setsnmp sys_locationは、System Locationを設定します

上記のコマンドで設定した値は、それぞれ以下のコマンドを使用して表示することができます。

- showsnmp snmp_port
- showsnmp trap_port
- showsnmp sys_contact
- showsnmp sys_name
- showsnmp sys_location.

コミュニティ

SNMPコミュニティを設定、表示、削除するには、CLIコマンドのsetsnmp snmp_community、list snmp_community、delete snmp_communityを使用します。

```
Intel 7110> setsnmp snmp_community
IP []:
Community String []:

Intel 7110> list snmp_community
SNMP Community List
IP:  x.x.x.x =>
String : public =>
Rights : read

Intel 7110> delete snmp_community

SNMP Community String(s) Deletion.

<2> Current Available SNMP Community String(s):

1.) IP:         0.0.0.0 => String:    public

2.) IP:         0.0.0.0 => String:   private

Enter number (1 to 2) to delete (q to quit) [1]: 2

Enter number (1 to 2) to delete (q to quit) [1]: q
```

重要 **IPの設定値として0.0.0.0を用いるとSNMPコンソールのIPの制限がなくなります(どのSNMPコンソールからもアクセスできるようになります)。**

トラップ・コミュニティ

トラップ・コミュニティを設定、表示、削除するには、CLIコマンドのsetsnmp trap_community、list trap_community、delete trap_communityを使用します。

```
Intel 7110> setsnmp trap_community
SNMP Trap Community String(s) Setting.
Enter a SNMP Trap Community IP (q to quit): 0.0.0.0
Enter a SNMP Trap Community String (q to quit): private
Enter a SNMP Trap Community IP (q to quit): 0.0.0.0
Enter a SNMP Trap Community String (q to quit): public
Enter a SNMP Trap Community IP (q to quit): q

Intel 7110> list trap_community
SNMP Trap Community String(s) information.
<2> Current SNMP Trap Community String(s):
1.) IP:   0.0.0.0 => String: public
2.) IP:   0.0.0.0 => String:  private

Intel 7110> delete trap_community
SNMP Trap Community String(s) Deletion.
<2> Current Available SNMP Trap Community String(s):

1.) IP:   0.0.0.0 => String:   public

2.) IP:   0.0.0.0 => String:   private

Enter number (1 to 2) to delete (q to quit) [1]: 2

Enter number (1 to 2) to delete (q to quit) [1]: q
```

アクセス制御

本装置は、blockコマンドおよびpermitコマンドを用意しています。このコマンドを使用すると、IP、IPマスク、ポート、ポート・マスクに基づいて、クライアントによるサーバへのアクセスを制御することができます。
IPおよびIPマスクを指定して、クライアントによる特定のサーバへのアクセスを禁止するには、以下に示すように、create blockコマンドを使用します。

blockの設定およびpermitの設定を表示、リスト、削除するには、第5章のコマンド・リファレンスを参照してください。

```
Intel 7110> create block
Client IP to block [0.0.0.0]: 10.1.2.1
Client IP mask [0.0.0.0]: 255.255.255.255
Server IP to block [0.0.0.0]: 20.1.2.1
Server IP mask [0.0.0.0]: 255.255.255.255
Server Port to block: 80
Server Port mask [0xffff]:<Enter>
```

IPおよびIPマスクを指定して、クライアントによる特定のサーバへのアクセスを許可するには、以下に示すように、create permitコマンドを使用します。

```
Intel 7110> create permit
Client IP [0.0.0.0]: 10.1.2.1
Client IP Mask [0.0.0.0]:255.255.255.255
Server IP [0.0.0.0]:20.1.2.1
Server IP Mask [0.0.0.0]:255.255.255.255
Server port [xx]: 443
Server port mask [0xffff]: <Enter>
```

permitの設定は有効なblock設定において、指定の通信に対するblockを無効にします(blockで設定した壁に穴を開けるようなイメージです)。

～Memo～