デバイスアクセスポリシー

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます：**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 *1*：機能の履歴

機能名	リリース情報	説明
SNMP および SSH のデバイスアクセスポリシー	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r	これは、トラフィックがインターフェイスを通過するために満たす必要のあるルールを定義する機能です。着信トラフィックのルールを定義した場合、そのルールが他のどのポリシーよりも先にトラフィックに適用されます。Cisco IOS XE Catalyst SD-WAN デバイス のコントロールプレーンは、一連の送信元からのローカルサービス（SSH や SNMP など）のデータトラフィックを処理します。オーバーレイを形成するには、ルーティングパケットが必要です。

• SSH に対する ACL ポリシーの確認 （8 ページ）

デバイスアクセスポリシーの概要

Cisco IOS XE SD-WAN リリース 17.2.1r 以降では、すべての Cisco IOS XE Catalyst SD-WAN デバイスでデバイスアクセスポリシーを設定するように Cisco SD-WAN Manager ユーザーインターフェイスが拡張されています。

Cisco IOS XE Catalyst SD-WAN デバイス のコントロールプレーンは、一連の送信元からのローカルサービス（SSH や SNMP など）のデータトラフィックを処理します。悪意のあるトラフィックを回避するため、フィルタを適用してデバイス アクセス トラフィックから CPU を保護することが重要です。

アクセスポリシーでは、トラフィックがインターフェイスを通過するために満たす必要のあるルールを定義します。着信トラフィックのルールを定義した場合、そのルールが他のどのポリシーよりも先にトラフィックに適用されます。ルーテッド ファイアウォール モードおよびトランスペアレント ファイアウォール モードで、アクセスポリシーを使用して IP トラフィックを制御できます。アクセスルールでは、使用されるプロトコル、送信元および宛先の IP アドレスまたはネットワーク、および任意でユーザーおよびユーザーグループに基づいてトラフィックが許可または拒否されます。インターフェイスでの各着信パケットは、指定した基準に基づいて転送またはドロップする必要があるかどうかを判断するために分析されます。発信トラフィックのアクセスルールを定義した場合、パケットはインターフェイスから出る前に分析されます。アクセスポリシーは順序で適用されます。つまり、デバイスは、ルールとパケットを比較するとき、アクセスポリシーリストの上から下に検索を行い、最初に一致したルールに対するポリシーを適用します。それ以降のルールは、（最初のルールより一致率が高くても）すべて無視されます。したがって、特定のルールがスキップされないようにするには、そのルールを汎用性の高いルールよりも上に配置する必要があります。

Cisco SD-WAN Manager を使用したデバイスアクセスポリシーの設定

Cisco IOS XE Catalyst SD-WAN デバイス は、コントロールプレーンに向けられた SNMP および SSH トラフィックを処理するためのデバイスアクセスポリシー設定をサポートしています。Cisco SD-WAN Manager を使用して、デバイスアクセスポリシーに基づいて宛先ポートを設定します。

（注） Cisco SD-WAN Manager の **[ツール（Tools）]** > **[SSHターミナル（SSH Terminal）]** からデバイスへの接続を許可するには、**デバイスアクセスプロトコル**を SSH として、**送信元データプレフィックス**を 192.168.1.5/32 として受け入れるルールを作成します。

ローカライズされたデバイスアクセス制御ポリシーを設定するには、Cisco SD-WAN Manager のポリシー構成ウィザードを使用します。

作成する特定のポリシーに応じて、特定のコンポーネントまたはすべてのコンポーネントを構成します。コンポーネントをスキップするには、[次へ（Next）] ボタンをクリックします。コンポーネントに戻るには、画面下部にある [戻る（Back）] ボタンをクリックします。

デバイスアクセスポリシーの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [ローカライズ型ポリシー（Localized Policy）] をクリックし、[カスタムオプション（Custom Options）] ドロップダウンの [ローカライズ型ポリシー（Localized Policy）] で [アクセス制御リスト（Access Control Lists）] を選択します。
3. [デバイスアクセスポリシーの追加（Add Device Access Policy）] ドロップダウンリストから、[IPv4デバイスアクセスポリシーの追加（Add IPv4 Device Access Policy）] または [IPv6デバイスアクセスポリシーの追加（Add IPv6 Device Access Policy）] オプションを選択してデバイスを追加します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降でポリシーシーケンスを使用せず、デフォルトアクションの [受け入れ（Accept）] または [ドロップ（Drop）] のみで IPv4 または IPv6 のデバイスアクセスポリシーを設定する場合、デバイスアクセスポリシーは SSH と SNMP 構成を作成します。デフォルトアクションのみを使用し、ポリシーシーケンスを使用せずにデバイスアクセスポリシーを作成して、SSH と SNMP の両方のデバイス設定または Cisco SD-WAN Manager 設定を作成できるようになりました。

SNMP サーバー構成を作成しない場合、デバイスアクセスポリシーによって作成された SNMP 構成は使用されません。

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 より前では、デフォルトアクションの [受け入れ（Accept）] または [ドロップ（Drop）] のみを使用し、ポリシーシーケンスを使用せずにデバイスアクセスポリシーを設定する場合、デバイスアクセスポリシーはデバイス設定または Cisco SD-WAN Manager 設定を作成しませんでした。

4. ドロップダウンリストから [IPv4デバイスアクセスポリシーの追加（Add IPv4 Device Access Policy）] を選択して、[IPv4 ACLポリシー（IPv4 ACL Policy）] を追加します。[デバイスIPv4 ACLポリシーの編集（Edit Device IPv4 ACL Policy）] ページが表示されます。
5. 新しいポリシーの名前と説明を入力します。
6. [ACLシーケンスの追加（Add ACL Sequence）] をクリックして、シーケンスを追加します。[デバイスアクセス制御リスト（Device Access Control List）] ページが表示されます。
7. [Sequence Rule] をクリックします。[マッチ（Match）] と [アクション（Actions）] オプションが表示されます。
8. [マッチ（Match）] をクリックし、ACL ポリシーの次の条件を選択して設定します。

一致条件	説明
デバイスアクセスプロトコル（Device Access Protocol）（必須）	ドロップダウンリストからキャリアを選択します。たとえば、SNMP、SSH などです。
送信元データプレフィクス（Source Data Prefix）	送信元 IP アドレスを入力します。たとえば、10.0.0.0/12 です。
送信元ポート	送信元ポートのリストを入力します。値の範囲は 0 ～ 65535 です。
Destination Data Prefix	宛先 IP アドレスを入力します。たとえば、10.0.0.0/12 です。
VPN	VPN ID を入力します。範囲は 0 ～ 65536 です。

9. [アクション（Actions）] をクリックし、ACL ポリシーの次の条件を設定します。

アクション条件	説明
承認	
カウンタ名	受け付けるカウンタ名を入力します。最大で 20 文字です。
削除（Drop）	
カウンタ名	ドロップするカウンタ名を入力します。最大で 20 文字です。

10. [マッチとアクションの保存（Save Match And Actions）] をクリックして、ACL ポリシーのすべての条件を保存します。

11. [デバイスアクセス制御リストポリシーの保存（Save Device Access Control List Policy）] をクリックして、選択したマッチ条件をアクションに適用します。

12. 一致するパケットがない場合、いずれかのルート ポリシー シーケンス ルールになります。左側のペインの [デフォルトアクション（Default Action）] では、パケットをドロップします。

（注） IPv6 プレフィックス一致は、Cisco IOS XE Catalyst SD-WAN デバイス ではサポートされていません。これらのデバイスで IPv6 プレフィックス一致を設定しようとすると、Cisco SD-WAN Manager はデバイス設定の生成に失敗します。

CLI を使用したデバイスアクセスポリシーの設定

Configuration:

```
ip access-list standard snmp-acl
 1 permit 10.0.1.12 255.255.255.0
 11 deny any
!

snmp-server community private view v2 ro snmp-acl

ip access-list extended ssh-acl
 1 permit tcp host 10.0.1.12 any eq 22
 11 deny tcp any any eq 22
!

line vty 0 4
 access-class ssh-acl in vrf-also
!
```

（注） IPv6 プレフィックス一致は、Cisco IOS XE Catalyst SD-WAN デバイス ではサポートされていません。

ACL 統計とカウンタの例

YANG を使用して ACL 統計とカウンタを設定するには、次の手順を実行します。

```
Yang file: Cisco-IOS-XE-acl-oper.yang

  grouping ace-oper-data {
    description
      "ACE operational data";
    leaf match-counter {
      type yang:counter64;
      description
        "Number of matches for an access list entry";
    }
  }
```

YANG モデルを使用した設定の例：

```
Router# show access-lists access-list ACL-1
ACCESS
CONTROL
LIST     RULE  MATCH
NAME     NAME  COUNTER
------------------------
ACL-1    1     0
         2     0

Router# show access-lists access-list ACL-1 | display xml
<config xmlns="http://tail-f.com/ns/config/1.0">
  <access-lists xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-acl-oper">
  <access-list>
    <access-control-list-name>ACL-1</access-control-list-name>
    <access-list-entries>
```

```
      <access-list-entry>
        <rule-name>1</rule-name>
        <access-list-entries-oper-data>
          <match-counter>0</match-counter>
        </access-list-entries-oper-data>
      </access-list-entry>
      <access-list-entry>
        <rule-name>2</rule-name>
        <access-list-entries-oper-data>
          <match-counter>0</match-counter>
        </access-list-entries-oper-data>
      </access-list-entry>
    </access-list-entries>
  </access-list>
  </access-lists>
</config>
Router#
```

CLI を使用して ACL 統計とカウンタを表示するには、次のように コマンドを使用します。

```
show ip access-list [access-list-number | access-list-name]
```

CLI を使用した統計の出力例：

```
show ip access-list [access-list-number | access-list-name]

Router# show ip access-list ACL-1
Extended IP access list ACL-1
10 permit ip host 10.1.1.1 any (3 matches) 30
30 permit ip host 10.2.2.2 any (27 matches)



To clear counters in ACL stats:

clear ip access-list counters {access-list-number | access-list-name}
```

SNMP サーバーに対する ACL ポリシーの確認

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r リリース以降、Cisco IOS XE Catalyst SD-WAN デバイス ではSNMPサーバーに対するデバイスアクセスポリシー機能をサポートしています。SNMP の場合、SNMP 機能テンプレートが設定されていないときに、Cisco SD-WAN Manager が確認をして、デバイスでテンプレートがプッシュされるのをブロックします。

（注） SNMP の場合、宛先データプレフィックスリストは Cisco IOS XE Catalyst SD-WAN デバイス に適用されません。デバイスの SNMP 設定を使用してこのローカライズ型ポリシーを適用しても、宛先データプレフィックスは無視されます。

Configuration:

```
snmp-server community private view v2 ro snmp-acl
```

snmp-server community コマンドの YANG モデル。以下は、YANG モデルの ACL 設定例を示したものです。

```
container community {
          description
            "Configure a SNMP v2c Community string and access privs";
          tailf:cli-compact-syntax;
          tailf:cli-sequence-commands;
          leaf community-string {
            tailf:cli-drop-node-name;
            type string;
          }
          container access {
            tailf:cli-drop-node-name;
            tailf:cli-flatten-container;
            leaf standard-acl {
              tailf:cli-drop-node-name;
              tailf:cli-full-command;
              type uint32 {
                range "1..99";
              }
            }
            leaf expanded-acl {
              tailf:cli-drop-node-name;
              tailf:cli-full-command;
              type uint32 {
                range "1300..1999";
              }
            }
            leaf acl-name {
              tailf:cli-drop-node-name;
              tailf:cli-full-command;
              type string;
            }
            leaf ipv6 {
              description
                "Specify IPv6 Named Access-List";
              tailf:cli-full-command;
              type string;
            }
            leaf ro {
              description
                "Read-only access with this community string";
              type empty;
            }
            leaf rw {
              description
                "Read-write access with this community string";
              type empty;
            }
          }
        }
```

以下は、snmp-server ACL 設定のサンプルテストログを示したものです。

```
Device# sh sdwan  ver
16.12.1

Device# config-t

admin connected from 127.0.0.1 using console on the device
Device(config)# snmp-server community TEST_1 RO 80
Device(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.

Device#
*Mar 13 21:17:19.377: %SYS-5-CONFIG_P: Configured programmatically by process
```

```
session_id_for_dmi_vty_100001 from console as NETCONF on vty31266
*Mar 13 21:17:19.377: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by
admin, transaction-id 518

Device#
Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80


Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80
Device#


admin connected from 127.0.0.1 using console on the device
Device(config)# snmp-server community TEST_V6 ipv6 acl-name-1
Device(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
Device#

*Mar 13 21:18:10.040: %SYS-5-CONFIG_P: Configured programmatically by process
session_id_for_dmi_vty_100001 from console as NETCONF on vty31266
*Mar 13 21:18:10.041: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by
admin, transaction-id 535

Device#
Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80
snmp-server community TEST_V6 ipv6 acl-name-1
Device#
Device# sh run | i snmp
snmp-server community TEST_1 RO 80
snmp-server community TEST_V6 RO ipv6 acl-name-1
Device#
```

SSH に対する ACL ポリシーの確認

Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r リリース以降、Cisco IOS XE Catalyst SD-WAN デバイス では仮想テレタイプ（VTY）回線を使用する SSH サーバー上で device-access-policy 機能をサポートしています。Cisco SD-WAN Manager は、バックエンドで使用可能なすべての VTY 回線を使用し、それに応じてポリシーをプッシュします。

Configuration:

```
line vty 0 4
 access-class ssh-acl in vrf-also
!
```

以下は、YANG モデルの ACL 設定例を示したものです。

```
// line * / access-class
    container access-class {
      description
        "Filter connections based on an IP access list";
      tailf:cli-compact-syntax;
      tailf:cli-sequence-commands;
      tailf:cli-reset-container;
      tailf:cli-flatten-container;
      list acccess-list {
        tailf:cli-drop-node-name;
```

```
        tailf:cli-compact-syntax;
        tailf:cli-reset-container;
        tailf:cli-suppress-mode;
        tailf:cli-delete-when-empty;
        key "direction";
        leaf direction {
          type enumeration {
            enum "in";
            enum "out";
          }
        }
        leaf access-list {
          tailf:cli-drop-node-name;
          tailf:cli-prefix-key;
          type ios-types:exp-acl-type;
          mandatory true;
        }
        leaf vrf-also {
          description
            "Same access list is applied for all VRFs";
          type empty;
        }
      }
    }
```

次に、line-server ACL 設定のサンプルテストログを示します。

```
Device# config-transaction

admin connected from 127.0.0.1 using console on Device
Device(config)# line vty 0 4
Device(config-line)# access-class acl_1 in vrf-also
Device(config-line)# transport input ssh
Device(config-line)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
Device#
*May 24 20:51:02.994: %SYS-5-CONFIG_P: Configured programmatically by process
iosp_vty_100001_dmi_nesd from console as NETCONF on vty31266
*May 24 20:51:02.995: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by
admin, transaction-id 227
Device#
Device#
Device# sh sdwan run | sec vty
Error: Licensing infrastructure is NOT initialized.
Error: Licensing infrastructure is NOT initialized.
line vty 0 4
 access-class acl_1 in vrf-also
 login local
 transport input ssh
line vty 5 80
 login local
 transport input ssh
Device#
Device# sh run | sec vty
Error: Licensing infrastructure is NOT initialized.
Error: Licensing infrastructure is NOT initialized.
line vty 0 4
 access-class acl_1 in vrf-also
 exec-timeout 0 0
 password 7 11051807
 login local
 transport preferred none
 transport input ssh
line vty 5 80
```

```
login local
transport input ssh
```

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。