



ACL Syslog 関連

アクセスコントロールリスト (ACL) Syslog 関連機能では、アクセスコントロールエントリ (ACE) Syslog エントリにタグ (ユーザ定義の Cookie またはデバイスが生成した MD5 ハッシュ値) を追加します。このタグは Syslog エントリを生成した ACL 内で ACE を一意に特定します。

- [機能情報の確認 \(1 ページ\)](#)
- [ACL Syslog 関連の前提条件 \(1 ページ\)](#)
- [ACL Syslog 関連に関する情報 \(2 ページ\)](#)
- [ACL Syslog 関連の設定方法 \(3 ページ\)](#)
- [ACL Syslog 関連の設定例 \(10 ページ\)](#)
- [IPv6 IOS ファイアウォールの追加情報 \(11 ページ\)](#)
- [ACL Syslog 関連に関する機能情報 \(12 ページ\)](#)

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ACL Syslog 関連の前提条件

ACL Syslog 関連機能を設定する前に、「IP アクセス リストの概要」モジュールでその概念を理解する必要があります。

ACL Syslog 相関機能は、ユーザ定義の cookie またはデバイスで生成されるハッシュ値を syslog 内の ACE メッセージに追加します。ログ オプションが ACE に対してイネーブルになっている場合、これらの値は ACE メッセージにのみ追加されます。

ACL Syslog 相関に関する情報

ACL Syslog 相関タグ

ACL Syslog 相関機能では、アクセス コントロール エントリ (ACE) Syslog エントリにタグ (ユーザ定義の Cookie またはデバイスが生成した MD5 ハッシュ値) を追加します。このタグは Syslog エントリを生成した ACE を一意に特定します。

ネットワーク管理ソフトウェアでは、どの ACE が特定の Syslog イベントを生成したかを特定するためにタグを使用できます。たとえば、ネットワーク管理者はネットワーク管理アプリケーションで ACE 規則を選択し、次にその ACE ルールに対応する Syslog イベントを表示できます。

Syslog メッセージにタグを追加するには、Syslog イベントを生成する ACE でログ オプションが有効になっている必要があります。システムは各メッセージに1つのタイプのタグ (ユーザ定義の Cookie またはデバイスで生成した MD5 ハッシュ値) のみを追加します。

ユーザ定義の Cookie タグを指定するには、ユーザは ACE ログ オプションを構成する際に Cookie 値を入力する必要があります。Cookie は英数字形式である必要があります。64 文字以上にはできず、16 進数表記 (0x など) で始めることはできません。

デバイスで生成した MD5 ハッシュ値タグを指定するには、ハッシュ生成機能をデバイスで有効にする必要があります。また、ACE ログ オプションを構成するときにユーザは Cookie 値を入力してはいけません。

ACE Syslog メッセージ

パケットが ACL 内のアクセス コントロール エントリ (ACE) と一致すると、そのイベントのログ オプションが有効になっているかどうかシステムでチェックされます。ログ オプションが有効な場合、ACL Syslog 相関機能がデバイスで構成されていると、システムは syslog メッセージにタグを付けます。タグは、標準情報に加えて syslog メッセージの最後に表示されます。

次は、ユーザ定義の Cookie タグを示すサンプル syslog メッセージです。

```
Jun 5 12:55:44.359: %SEC-6-IPACCESSLOGP: list logacl permitted tcp 192.168.16.1(38402)
-> 192.168.16.2(23), 1 packet [User_permitted_ACE]
```

次は、ハッシュ値タグを示すサンプル syslog メッセージです。

```
Jun 5 12:55:44.359: %SEC-6-IPACCESSLOGP: list logacl permitted tcp 192.168.16.1(38402)
-> 192.168.16.2(23), 1 packet [0x723E6E12]
```

ACL Syslog 関連の設定方法

デバイスでのハッシュ値生成の有効化

ユーザ定義 Cookie を使用して設定されていないシステム内でログをイネーブルにした各アクセスコントロールエントリ（ACE）の MD5 ハッシュ値を生成するデバイスを設定するには、このタスクを実行します。

ハッシュ値生成設定をイネーブルにすると、システムは既存のすべての ACE をチェックし、ハッシュ値を必要とする各 ACE のハッシュ値を生成します。ハッシュ値生成の設定をディセーブルにすると、これまでに生成されたすべてのハッシュ値がシステムから削除されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list logging hash-generation**
4. **end**
5. 次のいずれかを実行します。
 - **show ip access-list** *access-list-number*
 - **show ip access-list** *access-list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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 3	ip access-list logging hash-generation 例： Device(config)# ip access-list logging hash-generation	デバイスでハッシュ値生成を有効にします。 • ログを有効にした ACE があり、ハッシュ値を必要とする場合、デバイスは自動的に値を生成し、コンソールでその値を表示します。
ステップ 4	end 例：	(任意) グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device(config)# end	
ステップ 5	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> • show ip access-list <i>access-list-number</i> • show ip access-list <i>access-list-name</i> <p>例 :</p> <pre>Device# show ip access-list 101</pre> <p>例 :</p> <pre>Device# show ip access-list acl</pre>	<p>(任意) 番号付きまたは名前付き IP アクセス リストの内容を表示します。</p> <ul style="list-style-type: none"> • ログをイネーブルにした ACE のアクセス リストに生成したハッシュ値が含まれることを確認するには、出力を見直します。

デバイスでのハッシュ値生成の無効化

デバイスでのハッシュ値生成をディセーブルにするには、このタスクを実行します。ハッシュ値生成の設定をディセーブルにすると、これまでに生成されたすべてのハッシュ値がシステムから削除されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip access-list logging hash-generation**
4. **end**
5. 次のいずれかを実行します。
 - **show ip access-list** *access-list-number*
 - **show ip access-list** *access-list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>enable</p> <p>例 :</p> <pre>Device> enable</pre>	<p>特権 EXEC モードをイネーブルにします。</p> <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。
ステップ 2	<p>configure terminal</p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>

	コマンドまたはアクション	目的
ステップ 3	no ip access-list logging hash-generation 例 : <pre>Device(config)# no ip access-list logging hash-generation</pre>	デバイスでのハッシュ値生成をディセーブルにします。 <ul style="list-style-type: none"> • これまでに作成されたハッシュ値がシステムから削除されます。
ステップ 4	end 例 : <pre>Device(config)# end</pre>	(任意) グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	次のいずれかを実行します。 <ul style="list-style-type: none"> • show ip access-list <i>access-list-number</i> • show ip access-list <i>access-list-name</i> 例 : <pre>Device# show ip access-list 101</pre> 例 : <pre>Device# show ip access-list acl</pre>	(任意) IP アクセス リストの内容を表示します。 <ul style="list-style-type: none"> • ログをイネーブルにした ACE のアクセス リストに生成したハッシュ値が含まれないことを確認するには、出力を見直します。

ユーザ定義 Cookie を使用した ACL Syslog 相関の設定

syslog メッセージタグとしてユーザ定義の Cookie クッキーを使用し、特定のアクセス リストのデバイス上の ACL syslog 相関機能を設定するには、このタスクを実行します。

このセクションでは、番号付きアクセスリストのユーザ定義の Cookie を使用して、ACL Syslog 相関機能を設定する方法について例を示します。ただし、番号付きおよび名前付きアクセスリストの両方、標準および拡張アクセスリストの両方について、ユーザ定義の Cookie を使用し、ACL Syslog 相関機能を設定できます。



(注) 次の制限事項は、ユーザ定義の Cookie 値を選択する場合に適用されます。

- 最大文字数は 64 です。
- Cookie は 16 進表記 (0x など) で始めることはできません。
- Cookie は、**reflect**、**fragment**、**time-range** といったキーワードと同じまたはその一部を使用することはできません。たとえば、**reflect** と **ref** は無効な値です。ただし、これらのキーワードを先頭に使用することはできます。たとえば、**reflectedACE** と **fragment_33** は有効な値です。
- Cookie に設定できるのは英数字のみです。

>

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list access-list-number permit protocol source destination log word**
4. **end**
5. **show ip access-list access-list-number**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# 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 3	access-list access-list-number permit protocol source destination log word 例 : Device(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log UserDefinedValue	拡張 IP アクセス リストとユーザ定義の Cookie 値を定義します。 • Cookie 値の引数として <i>word</i> を入力します。
ステップ 4	end 例 :	(任意) グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device(config)# end	
ステップ 5	show ip access-list <i>access-list-number</i> 例 : Device# show ip access-list 101	(任意) IP アクセス リストの内容を表示します。 • 出力を見直して、アクセスリストにユーザ定義の Cookie 値が含まれることを確認します。

例

次に、ユーザ定義の Cookie 値を使用したアクセス リストに **show ip access-list** コマンドを使用した際の出力例を示します。

```
Device# show ip access-list
101
Extended IP access list 101
30 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = UserDefinedValue)
```

ハッシュ値を使用した ACL Syslog 関連の設定

syslog メッセージ タグとしてデバイスで生成されたハッシュ値を使用し、特定のアクセス リストのデバイス上の ACL Syslog 関連機能を設定するには、このタスクを実行します。

このセクションでは、番号付きアクセス リストのデバイスで生成されたハッシュ値を使用して、ACL Syslog 関連機能を設定する方法についてステップを示します。ただし、番号付きおよび名前付きアクセス リストの両方、標準および拡張アクセス リストの両方について、デバイスで生成されたハッシュ値を使用し、ACL Syslog 関連機能を設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list logging hash-generation**
4. **access-list *access-list-number* permit protocol source destination log**
5. **end**
6. **show ip access-list *access-list-number***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： Device# 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 3	ip access-list logging hash-generation 例： Device(config)# ip access-list logging hash-generation	デバイスでハッシュ値生成を有効にします。 <ul style="list-style-type: none"> ログを有効にした ACE があり、ハッシュ値を必要とする場合、デバイスは自動的に値を生成し、コンソールでその値を表示します。
ステップ 4	access-list access-list-number permit protocol source destination log 例： Device(config)# access-list 102 permit tcp host 10.1.1.1 host 10.1.1.2 log	拡張 IP アクセス リストを定義します。 <ul style="list-style-type: none"> アクセス リストのログ オプションを有効にしますが、Cookie 値は指定しないでください。 デバイスが、新たに定義したアクセスリストのハッシュ値を自動的に生成します。
ステップ 5	end 例： Device(config)# end	(任意) グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	show ip access-list access-list-number 例： Device# show ip access-list 102	(任意) IP アクセス リストの内容を表示します。 <ul style="list-style-type: none"> 出力を見直して、アクセスリストにルータが生成したハッシュ値が含まれることを確認します。

例

次に、デバイスで生成されたハッシュ値を使用したアクセスリストに **show ip access-list** コマンドを使用した際の実出力例を示します。

```
Device# show ip access-list
102
Extended IP access list 102
10 permit tcp host 10.1.1.1 host 10.1.1.2 log (hash = 0x7F9CF6B9)
```

ACL Syslog 関連タグ値の変更

ユーザ定義の Cookie の値を変更したり、ユーザ定義の Cookie とデバイスで生成したハッシュ値を置き換えたりするには、このタスクを実行します。

この手順は、番号付きアクセスリストの ACL Syslog 相関タグ値を変更する方法について示しています。ただし、番号付きおよび名前付きアクセスリストの両方と、標準および拡張アクセスリストの両方について、ACL Syslog 相関タグ値を変更できます。

手順の概要

1. **enable**
2. `show access-list`
3. **configure terminal**
4. `access-list access-list-number permit protocol source destination log word`
5. **end**
6. `show ip access-list access-list-number`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	<code>show access-list</code> 例： Device(config)# show access-list	(任意) アクセスリストの内容を表示します。
ステップ 3	configure terminal 例： Device# 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 4	<code>access-list access-list-number permit protocol source destination log word</code> 例： Device(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log NewUDV 例： OR 例： 例： Device(config)# access-list 101 permit tcp any any log replacehash	Cookie を修正したり、ハッシュ値を Cookie に変更したりします。 • アクセスリスト コンフィギュレーション コマンド全体を入力し、前のタグ値を新しいタグ値で置き換える必要があります。

	コマンドまたはアクション	目的
ステップ 5	end 例： Device(config)# end	(任意) グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	show ip access-list access-list-number 例： Device# show ip access-list 101	(任意) IP アクセス リストの内容を表示します。 • 変更を確認するために出力結果を見直します。

トラブルシューティングのヒント

アクセス リストのデバッグ情報を表示するには、**debug ip access-list hash-generation** コマンドを使用します。**debug** コマンドの出力例を次に示します。

```
Device# debug ip access-list hash-generation
Syslog hash code generation debugging is on
Device# show debug
IP ACL:
Syslog hash code generation debugging is on
Device# no debug ip access-list hash-generation

Syslog hash code generation debugging is off
Device# show debug
Device#
```

ACL Syslog 関連の設定例

例：ユーザ定義 Cookie を使用した ACL Syslog 関連の設定

次に、ユーザ定義 Cookie を使用して、デバイス上で ACL Syslog 関連機能を設定する方法について説明します。

```
Device#
Device# debug ip access-list hash-generation
Syslog MD5 hash code generation debugging is on
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# access-list 33 permit 10.10.10.6 log cook_33_std
Device(config)# do show ip access 33
Standard IP access list 33
10 permit 10.10.10.6 log (tag = cook_33_std)
Device(config)# end
```

例：ハッシュ値を使用した ACL Syslog 相関の設定

次の例では、デバイスで生成されたハッシュ値を使用して、デバイス上で ACL Syslog 相関機能を設定する方法について説明します。

```
Device# debug ip access-list hash-generation
Syslog MD5 hash code generation debugging is on
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# access-list 33 permit 10.10.10.7 log
Device(config)#
*Nov 7 13:51:23.615: %IPACL-HASHGEN: Hash Input: 33 standard permit 10.10.10.7
Hash Output: 0xCE87F535
Device(config)#
do show ip access 33

Standard IP access list 33
 10 permit 10.10.10.6 log (tag = cook_33_std)
 20 permit 10.10.10.7 log (hash = 0xCE87F535)
```

例：ACL Syslog 相関タグ値の変更

次に、既存のアクセスリストのユーザ定義 Cookie と新しい Cookie 値を交換する方法と、デバイス生成ハッシュ値とユーザ定義 Cookie 値を交換する方法について示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# do show ip access-list 101
Extended IP access list 101
 10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = MyCookie)
 20 permit tcp any any log (hash = 0x75F078B9)
Device(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log NewUDV
Device(config)# do show access-list
Extended IP access list 101
 10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = NewUDV)
 20 permit tcp any any log (hash = 0x75F078B9)
Device(config)# access-list 101 permit tcp any any log replacehash
Device(config)# do show access-list
Extended IP access list 101
 10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = NewUDV)
 20 permit tcp any any log (tag = replacehash)
```

IPv6 IOS ファイアウォールの追加情報

関連資料

関連項目	マニュアルタイトル
Cisco IOS コマンド	Cisco IOS Master Command List, All Releases

関連項目	マニュアル タイトル
セキュリティ コマンド	<ul style="list-style-type: none"> 『Cisco IOS Security Command Reference: Commands A to C』 『Cisco IOS Security Command Reference: Commands D to L』 『Cisco IOS Security Command Reference: Commands M to R』 『Cisco IOS Security Command Reference: Commands S to Z』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
IPv6 アドレッシングと接続	『IPv6 Configuration Guide』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

標準/RFC	タイトル
IPv6 に関する RFC	IPv6 RFCs

テクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ACL Syslog 相関に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1: ACL Syslog 相関に関する機能情報

機能名	リリース	機能情報
ACL Syslog 相関	Cisco IOS XE リリース 3.6S	ACL Syslog 相関機能は、ACE Syslog エントリにタグ（ユーザ定義の Cookie またはデバイスが生成した MD5 ハッシュ値）を追加します。このタグは Syslog エントリを生成した ACL 内で ACE を一意に特定します。

