



## CHAPTER 2

# ACE へのリモート アクセスのイネーブル化

この章では、Secure Shell (SSH; セキュア シェル) または Telnet プロトコルを使用してリモート接続を確立し、Cisco 4700 Series Application Control Engine (ACE) アプライアンス へのリモート アクセスを設定する方法について説明します。SSH からユーザ コンテキストに直接アクセスできるように、ACE を設定する方法についても説明します。また、ホストからの ICMP メッセージを受信するように ACE を設定する方法についても説明します。

この章の内容は、次のとおりです。

- [リモート アクセス設定のクイック スタート](#)
- [リモート ネットワーク管理トラフィック サービスの設定](#)
- [Telnet 管理セッションの設定](#)
- [SSH 管理セッションの設定](#)
- [アクティブなユーザ セッションの終了](#)
- [ACE に対する ICMP メッセージのイネーブル化](#)
- [SSH を介したユーザ コンテキストへの直接アクセス](#)
- [リモート アクセスの設定例](#)
- [セッション情報の確認](#)



(注)

ACE 前面のコンソール ポートに接続された専用端末を使用して直接接続を行い、端末表示属性を設定し、コンソールまたは仮想端末接続を使用して ACE にアクセスできるように端末回線を設定する方法については、[第 1 章「ACE の設定」](#)を参照してください。

# リモート アクセス設定のクイック スタート

表 2-1 に、ACE のリモート ネットワーク管理アクセスを設定するために必要な手順の概要を示します。各手順には、作業に必要な CLI コマンドが含まれています。

表 2-1 リモート ネットワーク管理設定のクイック スタート

---

## 作業およびコマンド例

---

1. 複数のコンテキストで動作する場合は、CLI プロンプトを観察して、適切なコンテキストで動作しているかどうかを確認してください。必要に応じて、適切なコンテキストに直接ログインするか、または切り替えてください。

```
host1/Admin# changeto C1
host1/C1#
```

これ以降、この表の例では、特に指定しないかぎり管理コンテキストを使用します。コンテキスト作成の詳細については、『Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide』を参照してください。

---

2. 設定モードを入力します。

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#
```

---

3. ネットワーク管理プロトコル（SSH または Telnet）およびクライアント送信元 IP アドレスに基づいて、ACE でネットワーク管理トラフィックを受信できるように許可するクラス マップを作成します。

```
host1/Admin(config)# class-map type management match-all
SSH-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol ssh source-address
172.16.10.0 255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
host1/Admin(config)# class-map type management match-all
TELNET-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol telnet
source-address 172.16.10.0 255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

---

表 2-1 リモート ネットワーク管理設定のクイック スタート (続き)

---

**作業およびコマンド例**

---

4. SSH および Telnet 管理プロトコル分類をアクティブにするポリシー マップを設定します。

```
host1/Admin(config)# policy-map type management first-match  
REMOTE_MGMT_ALLOW_POLICY  
host1/Admin(config-pmap-mgmt)# class SSH-ALLOW_CLASS  
host1/Admin(config-pmap-mgmt-c)# permit  
host1/Admin(config-pmap-mgmt-c)# exit  
host1/Admin(config-pmap-mgmt)# class TELNET-ALLOW_CLASS  
host1/Admin(config-pmap-mgmt-c)# permit  
host1/Admin(config-pmap-mgmt-c)# exit  
host1/Admin(config-pmap-mgmt)# exit  
host1/Admin(config)#
```

5. 単一 VLAN インターフェイスにトラフィック ポリシーを接続するか、または同じコンテキスト内のすべての VLAN インターフェイスにグローバルに接続します。たとえば、特定のインターフェイス VLAN を指定し、リモート管理ポリシー マップを適用するには、次のように入力します。

```
host1/Admin(config)# interface vlan 50  
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0  
host1/Admin(config-if)# service-policy input  
REMOTE_MGMT_ALLOW_POLICY  
host1/Admin(config-if)# exit
```

6. (任意) コンテキストごとに許可された Telnet セッションの最大数を設定します。

```
host1/Admin(config)# telnet maxsessions 3
```

7. (任意) コンテキストごとに許可された SSH セッションの最大数を設定します。

```
host1/Admin(config)# ssh maxsessions 3
```

---

表 2-1 リモート ネットワーク管理設定のクイック スタート (続き)

## 作業およびコマンド例

8. ユーザにグローバル管理権限がある場合は、**ssh key** コマンドを使用して、SSH サーバで使用される SSH 秘密鍵および対応する公開鍵を生成します。ホスト/鍵のペアは 1 つだけです。たとえば、管理コンテキストで RSA1 鍵ペアを生成するには、次のように入力します。

```
host1/Admin(config)# ssh key rsa1 1024
generating rsa1 key
.....
generated rsa1 key
```

9. (任意) フラッシュ メモリに設定変更を保存します。

```
host1/Admin(config)# exit
host1/Admin# copy running-config startup-config
```

## リモート ネットワーク管理トラフィック サービスの設定

ACE へのリモート アクセスに関する規則を設定するには、クラス マップ、ポリシー マップ、およびサービス ポリシーを使用します。ACE へのリモート ネットワーク管理アクセスを設定するうえで、各機能が果たす役割を簡単に説明します。

- クラス マップ - リモート ネットワーク トラフィックの一致基準を提供します。トラフィックを許可する場合の基準は、次のとおりです。
  - リモート アクセス ネットワーク管理プロトコル (SSH、Telnet、または ICMP)
  - クライアント送信元 IP アドレス
- ポリシー マップ - クラス マップで示された基準と一致するトラフィック分類に関して、リモート ネットワーク管理アクセスをイネーブルにします。
- サービス ポリシー - ポリシー マップをアクティブにして、インターフェイスにトラフィック ポリシーを接続するか、またはすべてのインターフェイス上でグローバルに接続します。

ここでは、リモート ネットワーク アクセス用のクラス マップ、ポリシー マップ、およびサービス ポリシーの作成方法について概要を示します。

ACE との Telnet および SSH リモート アクセス セッションは、コンテキスト単位で確立されます。ユーザおよびコンテキストの作成方法については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

ここで説明する内容は、次のとおりです。

- リモート管理クラス マップの作成および設定
- レイヤ 3 およびレイヤ 4 リモート アクセス ポリシー マップの作成
- サービス ポリシーの適用

## リモート管理クラス マップの作成および設定

レイヤ 3 およびレイヤ 4 クラス マップを作成して、ACE で受信されるリモート ネットワーク管理トラフィックを分類するには、**class-map type management** コンフィギュレーション モード コマンドを使用します。このコマンドを使用すると、一致基準として ACE が受信できる着信 IP プロトコル、およびクライアント送信元 IP アドレスやサブネット マスクを識別して、ACE でネットワーク管理トラフィックを受信できるようになります。**type management** キーワードは、SSH、Telnet、ICMP などのプロトコルのセキュリティを管理するために使用できるネットワーク トラフィックを定義します。

クラス マップには複数の **match** コマンドを指定できます。クラス マップを設定すると、複数の管理プロトコルおよび送信元 IP アドレスの **match** コマンドを特定のグループ内に定義して、このグループをトラフィック ポリシーに関連付けることができます。**match-all** および **match-any** キーワードによって、クラス マップに複数の一致条件が存在する場合に、ACE が複数の **match** 文演算をどのように評価するかが決まります。

このコマンドの構文は、次のとおりです。

```
class-map type management [match-all | match-any] map_name
```

キーワード、引数、およびオプションは次のとおりです。

- **match-all | match-any** - (任意) クラス マップ内に一致基準が複数存在する場合に、ACE でのレイヤ 3 およびレイヤ 4 ネットワーク管理トラフィックの評価方法を定義します。クラス マップは、**match** コマンドが次の条件の 1 つを満たした場合に、一致と見なされます。
  - **match-all** - (デフォルト) クラス マップに示されたすべての一致基準が満たされている場合、クラス マップ内のネットワーク トラフィック クラスと一致します (通常は、同じタイプの **match** コマンド)。
  - **match-any** - クラス マップに示された一致基準のいずれか 1 つが満たされている場合、クラス マップ内のネットワーク トラフィック クラスと一致します (通常は、さまざまなタイプの **match** コマンド)。
- **map\_name** - クラス マップに割り当てられた名前を指定します。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

CLI はクラス マップ管理コンフィギュレーション モードを開始します。ACE で受信されるリモート ネットワーク管理トラフィックを分類するには、**match protocol** コマンドを 1 つまたは複数含めて、クラス マップの一致基準を設定します。

たとえば、IP アドレス 172.16.10.0 から ACE に SSH および Telnet アクセスを許可するには、次のように入力します。

```
host1/Admin(config)# class-map type management match-all
SSH-TELNET_ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol ssh source-address
172.16.10.0 255.255.255.254
host1/Admin(config-cmap-mgmt)# match protocol telnet source-address
172.16.10.0 255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

ACE からレイヤ 3 およびレイヤ 4 ネットワーク管理クラス マップを削除する場合は、次のように入力します。

```
host1/Admin(config)# no class-map type management match-all
SSH-TELNET_ALLOW_CLASS
```

ここで説明する内容は、次のとおりです。

- [クラス マップの説明の定義](#)
- [リモート ネットワーク管理プロトコルの一致基準の定義](#)

## クラス マップの説明の定義

レイヤ 3 およびレイヤ 4 リモート管理クラス マップに関する概要を設定するには、クラス マップ コンフィギュレーション モードで **description** コマンドを使用します。

このコマンドの構文は、次のとおりです。

### **description** *text*

240 文字以内の英数字からなるテキスト スtring を、引用符で囲まず入力するには、*text* 引数を指定します。

たとえば、クラス マップの目的がリモート Telnet アクセスの許可であるという説明を指定するには、次のように入力します。

```
host1/Admin(config)# class-map type management TELNET-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow Telnet access to the
ACE
```

クラス マップから説明を削除する場合は、次のように入力します。

```
host1/Admin(config-cmap-mgmt)# no description
```

## リモート ネットワーク管理プロトコルの一致基準の定義

ACE が受信できるリモート ネットワーク アクセス管理プロトコルを識別するクラス マップを設定するには、クラス マップ コンフィギュレーション モードで **match protocol** コマンドを使用します。対応するポリシー マップを設定して、指定された管理プロトコルに ACE へのアクセスを許可します。ネットワーク管理アクセス トラフィック分類の一部として、クライアント送信元ホストの IP アドレスおよびサブネット マスクも一致条件として指定するか、またはあらゆるクライアント送信元アドレスを管理トラフィック分類で許可するように ACE に指示します。

このコマンドの構文は、次のとおりです。

```
[line_number] match protocol {http | https | icmp | kalap-udp | snmp
| ssh | telnet | xml-https} {any | source-address ip_address mask}
```

- *line\_number* - (任意) 個別の **match** コマンドの編集または削除を支援します。行番号として 2 ~ 255 の整数を入力します。**no line\_number** を入力すると、行全体を入力しなくても、長い **match** コマンドを削除できます。行番号は、**match** 文のプライオリティまたは順番を示すものではありません。

- **http** - Hypertext Transfer Protocol (HTTP; ハイパーテキスト転送プロトコル) を指定します。HTTP 管理プロトコルの設定については、第 8 章「XML インターフェイスの設定」を参照してください。
- **https** - セキュアな (SSL) ハイパーテキスト転送プロトコル (HTTP) を指定します。HTTPS 管理プロトコルの設定については、第 8 章「XML インターフェイスの設定」を参照してください。
- **https** - ポート 443 上で ACE のデバイス マネージャ GUI と接続するためのセキュアな (SSL) ハイパーテキスト転送プロトコル (HTTP) を指定します。
- **icmp** - ACE への Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) メッセージを指定します。ICMP 管理プロトコルの設定については、「ACE に対する ICMP メッセージのイネーブル化」を参照してください。
- **kalap-udp** - KAL-AP over UDP を使用した管理アクセスを指定します。KAL-AP 管理アクセスの設定については、『Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide』の「Configuring Health Monitoring」を参照してください。
- **snmp** - SNMP (簡易ネットワーク管理プロトコル) を指定します。SNMP 管理プロトコルの設定については、第 7 章「SNMP の設定」を参照してください。
- **ssh** - ACE との SSH リモート接続を指定します。ACE は、SSH バージョン 1 で提供されている SSH リモート シェル機能、および DES と 3DES 暗号をサポートしています。SSH 管理プロトコルの設定については、「SSH 管理セッションの設定」を参照してください。



---

(注) SSH v1.x および v2 は完全に別のプロトコルであり、互換性はありません。ACE にアクセスする場合は、必ず SSH v1.x クライアントを使用してください。

---

- **telnet** - ACE との Telnet リモート接続を指定します。Telnet 管理プロトコルの設定については、「Telnet 管理セッションの設定」を参照してください。
- **xml-https** - HTTPS を転送プロトコルとして指定し、ACE と Network Management System (NMS; ネットワーク管理システム) の間で XML ドキュメントの送信および受信を行います。通信は、ポート 10443 を使用して行われます。XML を利用する場合の HTTPS 管理プロトコルの使用については、第 8 章「XML インターフェイスの設定」を参照してください。





(注) レイヤ 3 およびレイヤ 4 ネットワーク管理クラス マップで **https** および **xml-https** の両方をイネーブルにできます。

- **any** - 管理トラフィック分類にあらゆるクライアント送信元アドレスを指定します。
- **source-address** - ネットワーク トラフィック一致条件として、クライアント送信元ホストの IP アドレスおよびサブネット マスクを指定します。分類の一部として、ACE は暗黙的に、ポリシー マップが適用されるインターフェイスから宛先 IP アドレスを取得します。
- **ip\_address** - クライアントの送信元 IP アドレス。IP アドレスはドット付き 10 進表記 (192.168.11.1 など) で入力します。
- **mask** - ドット付き 10 進表記のクライアントのサブネット マスク (255.255.255.0 など)。

たとえば、クラス マップで、送信元 IP アドレス 192.168.10.1 255.255.255.0 から ACE への SSH アクセスを許可するように指定する場合は、次のように入力します。

```
host1/Admin(config)# class-map type management SSH-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol ssh source-address
192.168.10.1 255.255.255.0
```

クラス マップから特定のネットワーク管理プロトコル一致条件を選択解除する場合は、次のように入力します。

```
host1/Admin(config-cmap-mgmt)# no match protocol ssh source-address
192.168.10.1 255.255.255.0
```

## レイヤ 3 およびレイヤ 4 リモート アクセス ポリシー マップの作成

レイヤ 3 および 4 トラフィック分類では、ACE で受信されるネットワーク管理トラフィックを設定するためのアクションを含む、レイヤ 3 およびレイヤ 4 ポリシー マップを作成します。ここでは、レイヤ 3 およびレイヤ 4 ネットワークトラフィック ポリシーの一般的な設定手順について概要を示します。内容は、次のとおりです。

- ACE で受信する SNMP ネットワーク管理トラフィック用レイヤ 3 およびレイヤ 4 ポリシー マップの作成
- レイヤ 3 およびレイヤ 4 ポリシー マップの説明の定義
- トラフィック ポリシーでのレイヤ 3 およびレイヤ 4 トラフィック クラスの指定
- レイヤ 3 およびレイヤ 4 管理トラフィックのポリシー アクションの定義

### ACE で受信する SNMP ネットワーク管理トラフィック用レイヤ 3 およびレイヤ 4 ポリシー マップの作成

レイヤ 3 およびレイヤ 4 ポリシー マップを設定し、ACE で受信される IP 管理トラフィックに適用されるさまざまなアクションを定義するには、**policy-map type management first-match** コンフィギュレーション コマンドを使用します。ACE は、ポリシー マップと最初に一致した分類を満たすトラフィックにのみ、指定されたアクションを実行します。ACE は、それ以上のアクションは実行しません。

このコマンドの構文は、次のとおりです。

```
policy-map type management first-match map_name
```

*map\_name* 引数では、レイヤ 3 およびレイヤ 4 ネットワーク管理ポリシー マップに割り当てる名前を指定します。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

このコマンドを使用するときには、ポリシー マップ管理コンフィギュレーション モードにアクセスします。

レイヤ 3 およびレイヤ 4 ネットワークトラフィック管理ポリシー マップを作成する場合の入力例を示します。

```
host1/Admin(config) # policy-map type management first-match  
REMOTE_MGMT_ALLOW_POLICY  
host1/Admin(config-pmap-mgmt) #
```

ACE からポリシー マップを削除する場合は、次のように入力します。

```
host1/Admin(config) # no policy-map type management first-match  
REMOTE_MGMT_ALLOW_POLICY
```

## レイヤ 3 およびレイヤ 4 ポリシー マップの説明の定義

レイヤ 3 およびレイヤ 4 リモート管理ポリシー マップに関する概要を設定するには、ポリシー マップ コンフィギュレーション モードで **description** コマンドを使用します。

このコマンドの構文は、次のとおりです。

### **description** *text*

*text* 引数は、設定する説明を指定します。240 文字以内の英数字からなるテキスト スtring を、引用符で囲まず入力します。

たとえば、ポリシー マップの目的がリモート Telnet アクセスの許可であるという説明を指定するには、次のように入力します。

```
host1/Admin(config-pmap-mgmt) # description Allow Telnet access to the  
ACE
```

ポリシー マップから説明を削除するには、次のように入力します。

```
host1/Admin(config-pmap-mgmt) # no description
```

## トラフィック ポリシーでのレイヤ 3 およびレイヤ 4 トラフィック クラスの指定

**class-map** コマンドを使用して作成されたレイヤ 3 およびレイヤ 4 トラフィック クラスを指定して、ネットワーク トラフィックにトラフィック ポリシーを関連付けるには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用します。このコマンドを使用すると、ポリシー マップ管理クラス コンフィギュレーション モードが開始します。

このコマンドの構文は、次のとおりです。

```
class {name1 [insert-before name2] | class-default}
```

引数、キーワード、およびオプションは次のとおりです。

- **name1 - class-map** コマンドを使用して設定された、定義済みのレイヤ 3 およびレイヤ 4 トラフィック クラスの名前。トラフィックをトラフィック ポリシーに関連付けるために使用されます。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
- **insert-before name2** - (任意) ポリシー マップ コンフィギュレーションの *name2* 引数で指定された、既存のクラス マップまたはインライン一致条件の前に、現在のクラス マップを配置します。ACE では、コンフィギュレーションの一部として順序の並べ替えを保存しません。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
- **class-default** - レイヤ 3 およびレイヤ 4 トラフィック ポリシー用に、**class-default** クラス マップを指定します。これは、ACE が作成する予約済みのクラス マップです。このクラスは削除したり変更したりできません。指定されたクラス マップの他の一致条件と一致しなかったすべてのネットワーク トラフィックは、デフォルトのトラフィック クラスに割り当てられます。指定された分類がいずれも一致しなかった場合、ACE は **class class-default** コマンドで指定されたアクションと一致させます。**class-default** クラス マップには、暗黙の **match any** 文があり、これを使用してあらゆるトラフィック分類を一致させます。**class-default** クラス マップ内の暗黙的な **match any** 文は、すべてのトラフィックと一致します。

たとえば、レイヤ 3 およびレイヤ 4 リモートアクセス ポリシー マップ内で既存のクラス マップを指定する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# class L4_REMOTE_ACCESS_CLASS
host1/Admin(config-pmap-mgmt-c)#
```

**insert-before** コマンドを使用して、ポリシー マップ内での 2 つのクラス マップの順序を定義する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# class L4_SSH_CLASS insert-before  
L4_REMOTE_ACCESS_CLASS
```

レイヤ 3 およびレイヤ 4 トラフィック ポリシーに **class-default** クラス マップを指定する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# class class-default  
host1/Admin(config-pmap-mgmt-c)#
```

レイヤ 3 およびレイヤ 4 ポリシー マップからクラス マップを削除する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# no class L4_REMOTE_ACCESS_CLASS
```

## レイヤ 3 およびレイヤ 4 管理トラフィックのポリシー アクションの定義

レイヤ 3 およびレイヤ 4 クラス マップで示されたネットワーク管理トラフィックを ACE で受信または拒否できるようにするには、ポリシー マップ クラス コンフィギュレーション モードで次のように **permit** または **deny** コマンドを指定します。

- クラス マップで示されたリモート管理プロトコルを ACE で受信できるようにするには、ポリシー マップ クラス コンフィギュレーション モードで **permit** コマンドを使用します。
- クラス マップで示されたリモート管理プロトコルを ACE で受信できないようにするには、ポリシー マップ クラス コンフィギュレーション モードで **deny** コマンドを使用します。

たとえば、SSH、Telnet、および ICMP 接続を ACE で受信できるようにするレイヤ 3 およびレイヤ 4 リモート ネットワーク トラフィック管理ポリシー マップを作成するには、次のように入力します。

```
host1/Admin(config)# policy-map type management first-match  
REMOTE_MGMT_ALLOW_POLICY  
host1/Admin(config-pmap-mgmt)# class SSH-ALLOW_CLASS  
host1/Admin(config-pmap-mgmt-c)# permit  
host1/Admin(config-pmap-mgmt-c)# exit  
host1/Admin(config-pmap-mgmt)# class TELNET-ALLOW_CLASS  
host1/Admin(config-pmap-mgmt-c)# permit  
host1/Admin(config-pmap-mgmt-c)# exit  
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS  
host1/Admin(config-pmap-mgmt-c)# permit  
host1/Admin(config-pmap-mgmt-c)# exit
```

たとえば、ACE による ICMP 接続を制限するポリシー マップを作成するには、次のように入力します。

```
host1/Admin(config)# policy-map type management first-action
ICMP_RESTRICT_POLICY
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# deny
```

## サービス ポリシーの適用

次のタスクを実行する場合は、**service-policy** コマンドを使用します。

- 作成済みのポリシー マップを適用します。
- 特定の VLAN インターフェイスにトラフィック ポリシーを接続するか、または同じコンテキスト内のすべての VLAN インターフェイスにグローバルに接続します。
- インターフェイスの入力方向にトラフィック ポリシーを接続することを指定します。

**service-policy** コマンドは、インターフェイス コンフィギュレーション モードおよびコンフィギュレーション モードで使用できます。インターフェイス コンフィギュレーション モードでポリシー マップを指定すると、特定の VLAN インターフェイスにポリシー マップが適用されます。コンフィギュレーション モードでポリシー マップを指定すると、コンテキストに関連付けられているすべての VLAN インターフェイスにポリシーが適用されます。

このコマンドの構文は、次のとおりです。

### **service-policy input** *policy\_name*

キーワード、引数、およびオプションは次のとおりです。

- **input** - インターフェイスの入力方向にトラフィック ポリシーを付加するように指定します。トラフィック ポリシーによって、そのインターフェイスで受信されたすべてのトラフィックが評価されます。
- *policy\_name* - 作成済みの **policy-map** コマンドで設定された、定義済みポリシー マップの名前。名前は最大 40 文字の英数字です。

たとえば、特定のインターフェイス VLAN を指定し、リモート アクセス ポリシー マップを適用するには、次のように入力します。

```
host1/Admin(config)# interface vlan 50
```

```
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```

たとえば、特定のコンテキストに関連付けられたすべての VLAN にリモート アクセス ポリシー マップをグローバルに適用するには、次のように入力します。

```
host1/Admin(config)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```

特定のインターフェイスからリモート アクセス トラフィック ポリシーを解除するには、次のように入力します。

```
host1/Admin(config-if)# no service-policy input
REMOTE_MGMT_ALLOW_POLICY
```

特定のコンテキストに関連付けられたすべての VLAN からリモート アクセス トラフィック ポリシーをグローバルに解除するには、次のように入力します。

```
host1/Admin(config)# no service-policy input REMOTE_MGMT_ALLOW_POLICY
```

トラフィック ポリシーを解除するには、次のいずれかの方法を使用します。

- サービス ポリシーを最後に適用した VLAN インターフェイスから個別に
- 同じコンテキストのすべての VLAN インターフェイスからグローバルに

次回にトラフィック ポリシーが特定の VLAN インターフェイスに付加されるか、または同じコンテキスト内のすべての VLAN インターフェイスにグローバルに付加された場合、ACE は関連付けられたサービス ポリシー統計情報を自動的にリセットして、サービス ポリシー統計情報の新しい開始点を設定します。

サービス ポリシーを作成する場合は、次の注意事項および制限事項に留意してください。

- コンテキストでグローバルに適用されるポリシー マップは、コンテキスト内に存在するすべてのインターフェイスに内部的に適用されます。
- インターフェイス上でアクティブになったポリシーは、重複する分類およびアクションに関して、指定されているあらゆるグローバル ポリシーを上書きします。
- ACE では、1 つのインターフェイス上でアクティブにできるのは、特定機能タイプの 1 つのポリシーだけです。

すべてのポリシー マップまたは特定のレイヤ 3 およびレイヤ 4 のリモート ネットワーク トラフィック管理ポリシー マップに関するサービス ポリシー統計情報を表示するには、EXEC モードで **show service-policy** コマンドを使用します。

このコマンドの構文は、次のとおりです。

```
show service-policy [policy_name [detail]]
```

キーワード、オプション、および引数は次のとおりです。

- *policy\_name* - (任意) 現在使用中の (インターフェイスに適用されている) 既存ポリシー マップ。最大 64 文字の英数字からなる、引用符で囲まれていない文字列です。既存のポリシー マップの名前を入力しなかった場合は、ACE にすべてのポリシー マップに関する情報と統計値が表示されます。
- **detail** - (任意) より詳細なポリシー マップ統計およびステータス情報を表示します。



(注)

ACE は、該当する接続の終了後、**show service-policy** コマンドによって表示されるカウンタをアップデートします。

たとえば、REMOTE\_MGMT\_ALLOW\_POLICY ポリシー マップのサービス ポリシー統計情報を表示するには、次のように入力します。

```
host1/Admin# show service-policy REMOTE_MGMT_ALLOW_POLICY
Status      : ACTIVE
Description: Allow mgmt protocols
-----
Context Global Policy:
  service-policy: REMOTE_MGMT_ALLOW_POLICY
```

ポリシー マップのサービス ポリシー統計情報をクリアするには、**clear service-policy** コマンドを使用します。このコマンドの構文は、次のとおりです。

```
clear service-policy policy_name
```

*policy\_name* 引数には、現在使用中の (インターフェイスに適用されている) 既存ポリシー マップの ID を入力します。

たとえば、現在処理中のポリシー マップ REMOTE\_MGMT\_ALLOW\_POLICY の統計情報を消去するには、次のように入力します。

```
host1/Admin# clear service-policy REMOTE_MGMT_ALLOW_POLICY
```



# Telnet 管理セッションの設定

ACE は、管理コンテキストの同時 Telnet 管理セッションを最大で 16、各ユーザコンテキストの同時 Telnet 管理セッションを最大で 4 つサポートします。

コンテキストごとに許可された Telnet セッションの最大数を制御するには、コンフィギュレーション モードで **telnet maxsessions** コマンドを使用します。

ACE は、合計で最大 256 の同時 Telnet セッションをサポートします。

ACE の Telnet リモート アクセス セッションは、コンテキスト単位で確立されません。コンテキストを作成し、インターフェイスおよび IP アドレスを割り当てて、ACE にログインするには、Telnet を使用して、この IP アドレスに接続します。この機能を使用すると、ACE にアクセスする場合に、特定のコンテキストを指定できます。ユーザおよびコンテキストの作成方法については、『Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide』を参照してください。

このコマンドの構文は、次のとおりです。

## **telnet maxsessions max\_sessions**

*max\_sessions* 引数は、関連付けられたコンテキストで許可されている同時 Telnet セッションの最大数を設定します。有効範囲は、管理コンテキストの場合は 1～16、各ユーザコンテキストの場合は 1～4 です。デフォルトは 16（管理コンテキスト）および 4（ユーザコンテキスト）です。

たとえば、管理コンテキストの同時 Telnet セッションの最大数を 3 に設定するには、次のように入力します。

```
host1/Admin(config)# telnet maxsessions 3
```

管理コンテキストの Telnet セッション数をデフォルトの 16 に戻すには、次のように入力します。

```
host1/Admin(config)# no telnet maxsessions
```

# SSH 管理セッションの設定

ここで説明する内容は、次のとおりです。

- [SSH 管理セッションの最大数の設定](#)
- [SSH ホスト 鍵ペアの生成](#)

ACE の SSH リモートアクセスセッションは、コンテキスト単位で確立されません。コンテキストを作成し、インターフェイスおよび IP アドレスを割り当てて、ACE にログインするには、SSH を使用して、この IP アドレスに接続します。この機能を使用すると、ACE にアクセスする場合に、特定のコンテキストを指定できます。ユーザおよびコンテキストの作成方法については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

## SSH 管理セッションの最大数の設定

ACE は、管理コンテキストの同時 SSH 管理セッションを最大で 16、各ユーザコンテキストの同時 SSH 管理セッションを最大で 4 つサポートします。

コンテキストごとに許可された SSH セッションの最大数を制御するには、コンフィギュレーション モードで **ssh maxsessions** コマンドを使用します。ACE は、合計で最大 256 の同時 SSH セッションをサポートします。

このコマンドの構文は、次のとおりです。

```
ssh maxsessions max_sessions
```

*max\_sessions* 引数は、関連付けられたコンテキストで許可されている同時 SSH セッションの最大数を設定します。有効範囲は、管理コンテキストの場合は 1 ~ 16、各ユーザ コンテキストの場合は 1 ~ 4 です。デフォルトは 16（管理コンテキスト）および 4（ユーザ コンテキスト）です。

たとえば、管理コンテキストの同時 SSH セッションの最大数を 3 に設定するには、次のように入力します。

```
host1/Admin(config)# ssh maxsessions 3
```

管理コンテキストの Telnet セッション数をデフォルトの 16 に戻すには、次のように入力します。

```
host1/Admin(config)# no ssh maxsessions
```

## SSH ホスト 鍵ペアの生成

ACE は、秘密鍵と公開鍵のペアを使用してコンテキストの認証を実行する、SSH セッションを介したリモート ログインをサポートしています。DSA および RSA キーはペアで生成されます（公開鍵と秘密鍵が 1 つずつ）。この方式のリモート接続を使用する場合、生成された秘密鍵と公開鍵のペアを使用して、メッセージを暗号化および復号化することにより、セキュアな通信に参加します。

グローバル管理者は、管理コンテキストでキー生成を実行します。ACE に関連付けられたすべてのコンテキストで、共通のキーが共有されます。ホスト/鍵のペアは 1 つのみ存在します。



(注)

管理者、または管理コンテキストで許可された別のユーザは、EXEC モードで **changeto** コマンドを使用して、管理コンテキストに移動します。管理者は、管理コンテキストで許可されたすべての機能を実行できます。

SSH サービスを確立する前に、SSH ホスト キーのペアおよび適切なバージョンが存在することを確認します。SSH サービスでは、SSH バージョン 1 および 2 で使用するための 3 種類のキー ペアを使用できます。使用されている SSH クライアントバージョンに従って、SSH ホスト キー ペアを生成します。各キー ペアに指定されるビット数は、768 ~ 4096 です。

SSH サーバで使用する SSH 秘密鍵および対応する公開鍵を生成するには、コンフィギュレーション モードで **ssh key** コマンドを使用します。

このコマンドの構文は、次のとおりです。

```
ssh key {dsa | rsa | rsa1} [bits [force]]
```

引数、キーワード、およびオプションは次のとおりです。

- **dsa** - SSH バージョン 2 プロトコルに対応する DSA キー ペアを生成します。
- **rsa** - SSH バージョン 2 プロトコルに対応する RSA キー ペアを生成します。
- **rsa1** - SSH バージョン 1 プロトコルに対応する RSA1 キー ペアを生成します。
- **bits** - (任意) キー ペアのビット数を指定します。DSA の場合の範囲は 768 ~ 2048 です。RSA および RSA1 の場合の範囲は 768 ~ 4096 です。指定したビット数が多いほど、キーの生成に時間がかかります。デフォルトは 768 です。

## ■ アクティブなユーザセッションの終了

- **force** - (任意) 既存のキーが存在する場合も、DSA または RSA キーを強制的に生成します。必要なバージョンに対応した SSH キー ペア オプションがすでに生成されている場合に、前に生成したキー ペアを上書きするには、**force** オプションを使用します。

キーを生成する前に、ホスト名を設定します。この設定は、キーの生成に使用されます。ホスト名の設定方法は、第 1 章「ACE の設定」を参照してください。

たとえば、管理コンテキストで RSA1 キーペアを生成するには、次のように入力します。

```
host1/Admin(config)# ssh key rsa1 1024
generating rsa1 key
.....
generated rsa1 key
```

SSH ホスト キー ペアを削除するには、次のように入力します。

```
host1/Admin(config)# no ssh key rsa1
```

信頼できるすべてのホストの公開鍵を消去するには、**clear ssh hosts EXEC** コマンドを使用します。これらのキーは SSH サーバから SSH クライアントに送信されるか、または手動で入力します。ACE からの SSH 接続が確立されると、SSH クライアントは公開鍵を受け取り、ローカルに格納します。これらのキーをすべて消去するには、EXEC モードで **clear ssh hosts** コマンドを使用します。

## アクティブなユーザセッションの終了

アクティブ コンテキストのアクティブな SSH または Telnet セッションを終了するには、EXEC モードで次のいずれかのコマンドを使用します。

- **clear ssh {*session\_id* | hosts}**
- **clear telnet {*session\_id*}**

引数、キーワード、およびオプションは次のとおりです。

- **session\_id** - 切断する SSH または Telnet セッションの ID を指定します。具体的な **session\_id** 値を取得するには、EXEC モードで **show ssh session-info** コマンドまたは **show telnet** コマンドを使用します。詳細については、「SSH を介したユーザ コンテキストへの直接アクセス」を参照してください。
- **hosts** - ACE のコンフィギュレーションから、信頼できる SSH ホストのリストを消去します。

たとえば、SSH セッションを終了するには、次のように入力します。

```
host1/Admin # clear ssh 345
```

## ACE に対する ICMP メッセージのイネーブル化

ACE はデフォルトで、ACE インターフェイスでの ICMP メッセージの受信、または ACE インターフェイスを介した ICMP メッセージの送信を許可していません。ICMP はネットワーク接続をテストするための重要なツールですが、ネットワーク ハッカーが ICMP を使用して ACE またはネットワークを攻撃することもできます。初期テスト中は ICMP を許可し、通常操作中は禁止することを推奨します。

ICMP メッセージがホストから ACE に、または ACE から ICMP 応答を許可する必要のあるホストに送信される場合に、アドレスの ACE インターフェイスへの到達を許可または拒否するには、次のいずれかを設定します。

- クラス マップ - ACE の ICMP ネットワーク トラフィック一致基準を提供します。
- ポリシー マップ - ACE に対する ICMP ネットワーク管理アクセスをイネーブルにします。
- サービス ポリシー - ポリシー マップをアクティブにし、トラフィック ポリシーを特定のインターフェイスに付加するか、またはすべてのインターフェイスにグローバルに付加し、ポリシーの適用方向を指定します。

「リモート ネットワーク管理トラフィック サービスの設定」のネットワーク管理クラス マップ、ポリシー マップ、サービス ポリシーの設定方法については、ACEを参照してください。

ACE を介した ICMP メッセージの送信を許可するには、ICMP タイプ (echo、echo-reply、unreachable など) に基づいてネットワーク接続を許可または拒否するように ICMP ACL (アクセス コントロール リスト) を設定します。詳細については、『Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide』を参照してください。



(注)

ACE からホストへの ping のみを許可し (インターフェイスへのエコー返信を許可し)、ホストから ACE への ping を許可しない場合は、クラス マップおよびポリシー マップを定義しないで、ICMP アプリケーション プロトコル インスタクションをイネーブルにします。詳細については、『Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide』を参照してください。

## ■ SSH を介したユーザ コンテキストへの直接アクセス

たとえば、ACE の ICMP ping 受信を許可するには、次のように入力します。

```
host1/Admin(config)# class-map type management match-all
ICMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow ICMP packets
host1/Admin(config-cmap-mgmt)# match protocol icmp source-address
172.16.10.0 255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)# policy-map type management first-action
ICMP_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input ICMP_ALLOW_POLICY
```

## SSH を介したユーザ コンテキストへの直接アクセス

グローバル管理者は、管理コンテキストから、ユーザ コンテキストを設定したり、リモート SSH セッションからこのユーザ コンテキストへの直接ログインアクセスをイネーブルにしたりできます。SSH からユーザ コンテキストへの直接アクセスが可能となるように ACE を設定する手順は、次のとおりです。

**ステップ 1** 次のコマンドを入力して、ユーザ コンテキストを作成します。

```
host1/Admin(config)# context C1
host1/Admin(config-context)#
```

『Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide』を参照してください。

**ステップ 2** 既存の VLAN にユーザ コンテキストを関連付けて、コンテキストが自身に分類されたトラフィックを受信できるようにするには、次のコマンドを入力します。

```
host1/Admin(config-context)# allocate-interface vlan 100
```

『Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide』を参照してください。

**ステップ 3** 次のコマンドを入力して、SSH ホスト キー ペアを生成します。

```
host1/Admin(config-context)# ssh key rsa1 1024
generating rsa1 key
.....
generated rsa1 key
```

「SSH ホスト 鍵ペアの生成」を参照してください。

**ステップ 4** 次のコマンドを入力して、ステップ 1 で作成した C1 コンテキストに変更し、このコンテキストでコンフィギュレーション モードを開始します。

```
host1/Admin(config-context)# do changeto C1
host1/C1(config-context)# exit
host1/C1(config)#
```

**changeto** コマンドを使用できるのは、管理コンテキストで認証されたユーザのみです。

**ステップ 5** 次のコマンドを入力して、ステップ 2 のユーザ コンテキストに割り当てられた VLAN インターフェイスを設定します。

```
host1/C1(config)# interface vlan 50
host1/C1(config-if)# ip address 192.168.1.1 255.255.255.0
host1/C1(config-if)# no shutdown
host1/C1(config-if)# exit
host1/C1(config)#
```

たとえば、インターフェイスに IP アドレスを割り当て、**no shutdown** コマンドを使用して、コンテキスト内でインターフェイスを再イネーブルにします。  
『Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide』を参照してください。

**ステップ 6** 次のコマンドを入力して、SSH リモート管理ポリシーを作成し、関連付けられたサービス ポリシーをすべての VLAN インターフェイスに適用するか、またはユーザ コンテキストに割り当てられた VLAN インターフェイスにのみ適用します。

```
host1/C1(config)# class-map type management match-all SSH-ALLOW_CLASS
host1/C1(config-cmap-mgmt)# match protocol ssh source-address
172.16.10.0 255.255.255.254
host1/C1(config-cmap-mgmt)# exit
host1/C1(config)#
host1/C1(config)# policy-map type management first-match
REMOTE_MGMT_ALLOW_POLICY
host1/C1(config-pmap-mgmt)# class SSH-ALLOW_CLASS
host1/C1(config-pmap-mgmt-c)# permit
host1/C1(config-pmap-mgmt-c)# exit
host1/C1(config)# interface vlan 50
```

## リモートアクセスの設定例

```

host1/C1(config-if)# ip address 192.168.1.1 255.255.255.0
host1/C1(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
host1/C1(config-if)# exit
host1/C1(config)#

```

「リモート ネットワーク管理トラフィック サービスの設定」を参照してください。

**ステップ 7** 次のコマンドを入力して、IP ルートを作成します。

```

host1/C1(config)# ip route 0.0.0.0 255.255.255.0 192.168.4.8

```

『Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide』を参照してください。

---

SSH クライアントからユーザ コンテキストに直接アクセスする手順は、次のとおりです。

**ステップ 1** SSH クライアントから、ユーザ コンテキスト VLAN インターフェイスの IP アドレスへのリモート SSH セッションを確立します。

**ステップ 2** ユーザ コンテキスト VLAN インターフェイスのパスワードを入力します。ユーザ コンテキストの EXEC モードで、ACE CLI プロンプトが表示されます。

```

host1/C1#

```

## リモート アクセスの設定例

次に、クラス マップ、ポリシー マップ、およびサービス ポリシーを使用して、ACE へのリモート アクセスに関する規則を定義する実行コンフィギュレーションの例を示します。この例では、リモート アクセスの設定は太字で示されています。

```

telnet maxsessions 3

```

```

ssh maxsessions 3

```

```

access-list ACL1 line 10 extended permit ip any any

```



```
class-map type management match-any L4_REMOTE-MGT_CLASS
  description Allows Telnet, SSH, and ICMP protocols
  2 match protocol telnet any
  3 match protocol ssh any
  4 match protocol icmp any

policy-map type management first-match L4_REMOTE-MGT_POLICY
  class L4_REMOTE-MGT_CLASS
    permit

interface vlan 50
  ip address 192.168.1.1 255.255.255.0
  access-group input ACL1
  service-policy input L4_REMOTE-MGT_POLICY
  no shutdown

ssh key rsa1 1024 force
```

## セッション情報の確認

ここで説明する内容は、次のとおりです。

- [Telnet セッション情報の表示](#)
- [SSH セッション情報の表示](#)

## Telnet セッション情報の表示

Telnet セッションの関連情報を表示するには、EXEC モードで **show telnet** コマンドを使用します。特定のコンテキストに関連付けられた Telnet 情報を表示できるのは、コンテキスト管理者のみです。

このコマンドの構文は、次のとおりです。

```
show telnet [context_name]
```

オプションの *context\_name* 引数は、特定の Telnet セッション情報を表示するコンテキストの名前を指定します。*context\_name* 引数は、大文字と小文字を区別します。

入力例を示します。

```
host1/Admin# show telnet
```

表 2-2 に、**show telnet** コマンド出力に含まれるフィールドの説明を示します。

表 2-2 show telnet コマンドのフィールドの説明

フィールド	説明
SessionID	Telnet セッションの一意なセッション識別子。
Remote Host	リモート Telnet クライアントの IP アドレスとポート。
Active Time	ACE が Telnet 接続要求を受信してからの経過時間。

イネーブル化された Telnet セッションの最大数を表示するには、EXEC モードで **show telnet maxsessions** コマンドを使用します。特定のコンテキストに関連付けられた Telnet セッション情報を表示できるのは、コンテキスト管理者のみです。

このコマンドの構文は、次のとおりです。

```
show telnet maxsessions [context_name]
```

オプションの *context\_name* 引数は、Telnet セッションの最大数を表示するコンテキストの名前を指定します。*context\_name* 引数は、大文字と小文字を区別します。

入力例を示します。

```
host1/Admin# show telnet maxsessions
Maximum Sessions Allowed is 4
```

## SSH セッション情報の表示

ここで説明する内容は、次のとおりです。

- [SSH セッション情報の表示](#)
- [SSH キーの詳細の表示](#)

## SSH セッション情報の表示

SSH セッションの関連情報を表示するには、EXEC モードで **show ssh session-info** コマンドを使用します。特定のコンテキストに関連付けられた SSH セッション情報を表示できるのは、コンテキスト管理者のみです。

このコマンドの構文は、次のとおりです。

```
show ssh session-info [context_name]
```

オプションの *context\_name* 引数は、特定の SSH セッション情報を表示するコンテキストの名前を指定します。*context\_name* 引数は、大文字と小文字を区別します。

入力例を示します。

```
host1/Admin# show ssh session-info
```

表 2-3 に、**show ssh session-info** コマンド出力に含まれるフィールドの説明を示します。

表 2-3 ssh session info コマンドのフィールドの説明

フィールド	説明
SessionID	SSH セッションの一意なセッション識別子。
Remote Host	リモート SSH クライアントの IP アドレスとポート。
Active Time	ACE が SSH 接続要求を受信してからの経過時間。

イネーブル化された SSH セッションの最大数を表示するには、EXEC モードで **show ssh maxsessions** コマンドを使用します。特定のコンテキストに関連付けられた SSH セッション情報を表示できるのは、コンテキスト管理者のみです。

このコマンドの構文は、次のとおりです。

```
show ssh maxsessions [context_name]
```

オプションの *context\_name* 引数は、コンテキスト管理者が SSH セッションの最大数を表示するコンテキストの名前を指定します。*context\_name* 引数は、大文字と小文字を区別します。

入力例を示します。

```
host1/Admin# show ssh maxsessions  
Maximum Sessions Allowed is 4 (SSH Server is enabled)
```

## SSH キーの詳細の表示

指定されたキー、またはすべてのキー（キーを指定しない場合）のホスト キーペアの詳細を表示するには、EXEC モードで **show ssh key** コマンドを使用します。

このコマンドの構文は、次のとおりです。

```
show ssh key [dsa | rsa | rsa1]
```

引数、キーワード、およびオプションは次のとおりです。

- **dsa** - SSH バージョン 2 プロトコルに対応する DSA キー ペアを指定します。
- **rsa** - SSH バージョン 2 プロトコルに対応する RSA キー ペアを指定します。
- **rsa1** - SSH バージョン 1 プロトコルに対応する RSA1 キー ペアを指定します。

入力例を示します。

```
host1/Admin # show ssh key
*****
could not retrieve rsa1 key information
*****
rsa Keys generated:Tue Mar 7 19:37:17 2006

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEA4v4DQ8aN1482qDTRju9G07hEIXCgTWanPm+WOCU1kihZ
QNd5ZwA50CBAJSfIIIB4iED6iQbhOkbXSneCvTb5mVoish2wwJrETpIDIEGxxh/jWVsU/MeBbA/7o5tv
gCeT6p7pGF5oUNYFP0OeZ9BiIWDc4jBmYEQLEqJHPrMhSFE=

bitcount:1024
fingerprint:
f5:55:00:18:bc:af:41:74:b6:bc:aa:8e:46:31:74:4f
*****
dsa Keys generated:Tue Dec 20 19:37:17 2005

ssh-dss
AAAAB3NzaC1kc3MAAACBApQdDdEqU+0gNtKRXM+DQAXnvcB+H89nq8jA4WgJ7uQcuDCLaG7Lq
jtKTltJjA6aZVywsQWQ6n4kTlkavZy3cj6PUBSyqvmCTsaYyYo4UQ6CKrK9V+NsfgzTSLWTH8iDUvYjL
c3nU51QEKjy7mPsQeX31y1M1rhp8qhkBMKxkc49XAAAAFQCPM0QJrq6+kkaghJpeNxeXhUH9HwAAAIEA
keZ1ZJM6sfKqJDYPLHkTro+lpbV9uR4VyYoZmSoehi/LmSaZDq+Mc8UN1LM+i5vkOgnKcearD9lM4/hK
```

```
zZGYx5hJOiYCKj/ny2a5p/8HK152cnsOAg6ebkiTTWAprcWrcHDS/1mcaI5GzLrZCd1XW5
gBFZtMTJGs
tICmVWjibewAAACBAJQ66zdZQqYiCWtZfmakridEGDTLV6ixIDjBNgb84qlj+Y1XMzqLL0
D4oMSb7idE
L3BmhQYQW7hkTK0oS4kVawI1VmW2kvrqoGQnLNQRMvisAXuJWKK1Ln6vWPGZZe8KoALv0G
XxsOv2gk/z
TDk01oCaTVw//bXJtoVRgIlWXLIP
```

```
bitcount:1024
```

```
fingerprint:
```

```
8e:13:5c:3e:1a:9c:7a:ed:d0:84:eb:96:12:db:82:be
```

```
*****
```

■ セッション情報の確認