

Catalyst 9800ワイヤレスコントローラシリーズでの802.1X認証の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[WLC の設定](#)

[9800 WLCでのAAAの設定](#)

[WLANプロファイルの設定](#)

[ポリシープロファイルの設定](#)

[ポリシータグの設定](#)

[ポリシータグの割り当て](#)

[ISE の設定](#)

[ISEでのWLCの宣言](#)

[ISE での新しいユーザの作成](#)

[認証プロファイルの作成](#)

[ポリシーセットの作成](#)

[認証ポリシーの作成](#)

[承認ポリシーの作成](#)

[確認](#)

[トラブルシューティング](#)

[WLCでのトラブルシューティング](#)

[ISEでのトラブルシューティング](#)

概要

このドキュメントでは、Cisco Catalyst 9800シリーズワイヤレスコントローラで802.1Xセキュリティを使用してWLANを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 802.1X

使用するコンポーネント

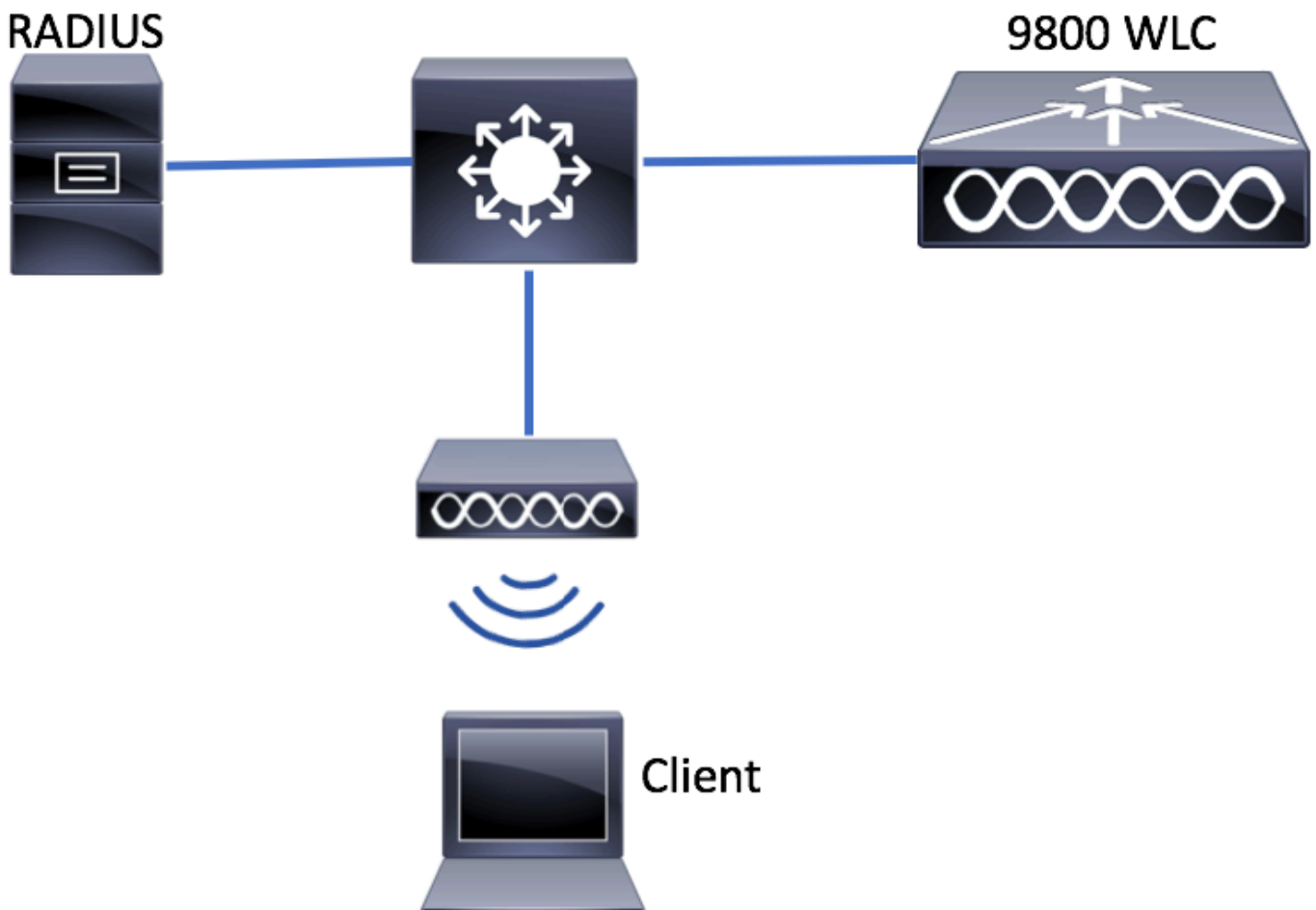
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 9800ワイヤレスコントローラシリーズ(Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE 3.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



WLC の設定

9800 WLCでのAAAの設定

GUI :

ステップ1:RADIUSサーバを宣言します。移動先 [Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add RADIUSサーバ情報](#)を入力します。

今後、中央Web認証(または認可変更(CoA)を必要とするあらゆる種類のセキュリティ)を使用する予定の場合は、CoAのサポートが有効になっていることを確認します。

Create AAA Radius Server ✕

Name*	<input type="text" value="ISE-kcg"/>	Clear PAC Key	<input type="checkbox"/>
IPV4/IPv6 Server Address*	<input type="text" value="172.16.0.11"/>	Set New PAC Key	<input type="checkbox"/>
Shared Secret*	<input type="password" value="....."/>		
Confirm Shared Secret*	<input type="password" value="....."/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		
Support for CoA	<input checked="" type="checkbox"/> ENABLED		

↶ Cancel

Save & Apply to Device

ステップ 2 : RADIUSサーバをRADIUSグループに追加します。移動先 Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add. グループに名前を付け、先ほど作成したサーバを次のリストに移動します。 Assigned Servers.

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

ステップ 3 : 認証方式リストを作成します。移動先 [Configuration > Security > AAA > AAA Method List > Authentication > + Add](#).

The screenshot shows the Cisco configuration interface. On the left is a dark sidebar menu with a search bar and four main categories: Dashboard, Monitoring, Configuration, and Administration. The 'Configuration' menu item is highlighted with a red box. On the right, the main content area is titled 'Authentication Authorization and Accounting'. Below the title is a blue '+ AAA Wizard' button. Underneath is a red-bordered box containing the text 'AAA Method List'. To the right of this box is the text 'Servers / Groups'. Below this is a 'General' section with a red-bordered box containing the text 'Authentication'. To the right of this is a blue '+ Add' button. Below the 'Authentication' section is an 'Authorization' section with a table header 'Name'.

次の情報を入力します。

Quick Setup: AAA Authentication

Method List Name* list-name

Type* dot1x

Group Type group

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

Cancel Save & Apply to Device

CLI :

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

AAAデッドサーバ検出に関する注意

RADIUSサーバを設定した後は、それが「ALIVE」と見なされているかどうかを確認できます。

```
#show aaa servers | s WNCN Platform State from WNCN (1) : current UP Platform State from WNCN
(2) : current UP Platform State from WNCN (3) : current UP Platform State from WNCN (4) :
current UP ...
```

この設定は、**dead criteria**、また、**deadtime WLC**で設定します。特に複数のRADIUSサーバを使用する場合に有効です。

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

注: **dead criteria** は、RADIUSサーバをデッドとしてマークするために使用される基準です。以下で構成される：1.コントローラが最後にRADIUSサーバから有効なパケットを受信してから、サーバがデッド状態としてマークされるまでの時間を表すタイムアウト (秒)。2.カウ

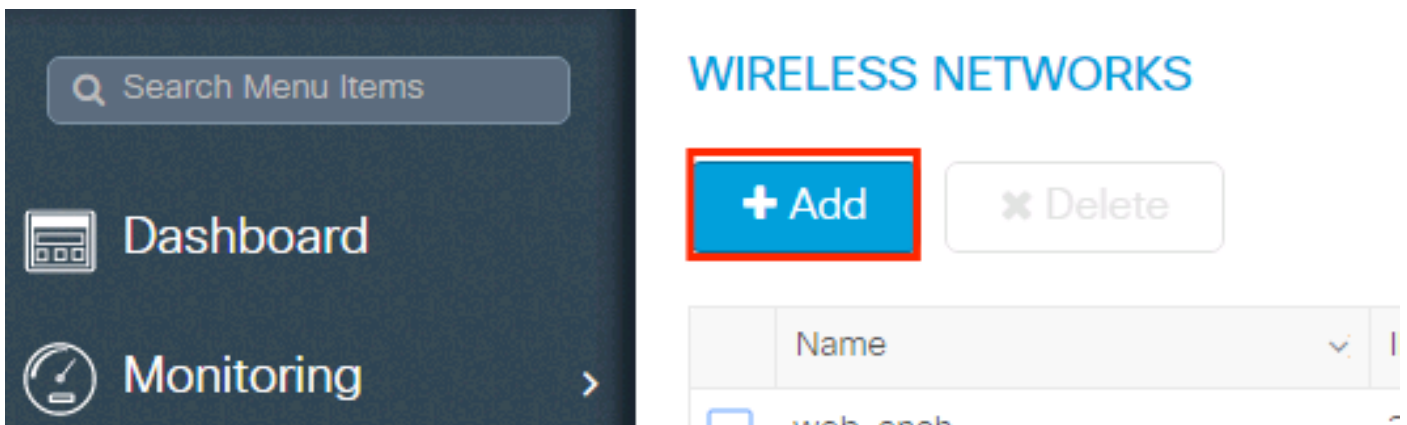
ンタ。RADIUSサーバがデッドとしてマークされるまでにコントローラで発生する必要がある連続タイムアウトの数を表します。

注: `deadtime dead-criteria`によってサーバがdeadとしてマークされた後、サーバがdeadステータスのままになる時間（分単位）を指定します。期限が切れると、コントローラはサーバをUP(ALIVE)としてマークし、登録クライアントに状態変更を通知します。状態がUPとマークされた後もサーバが到達不能であり、デッド基準が満たされる場合、サーバはデッドタイムインターバルの間に再びデッドとしてマークされます。

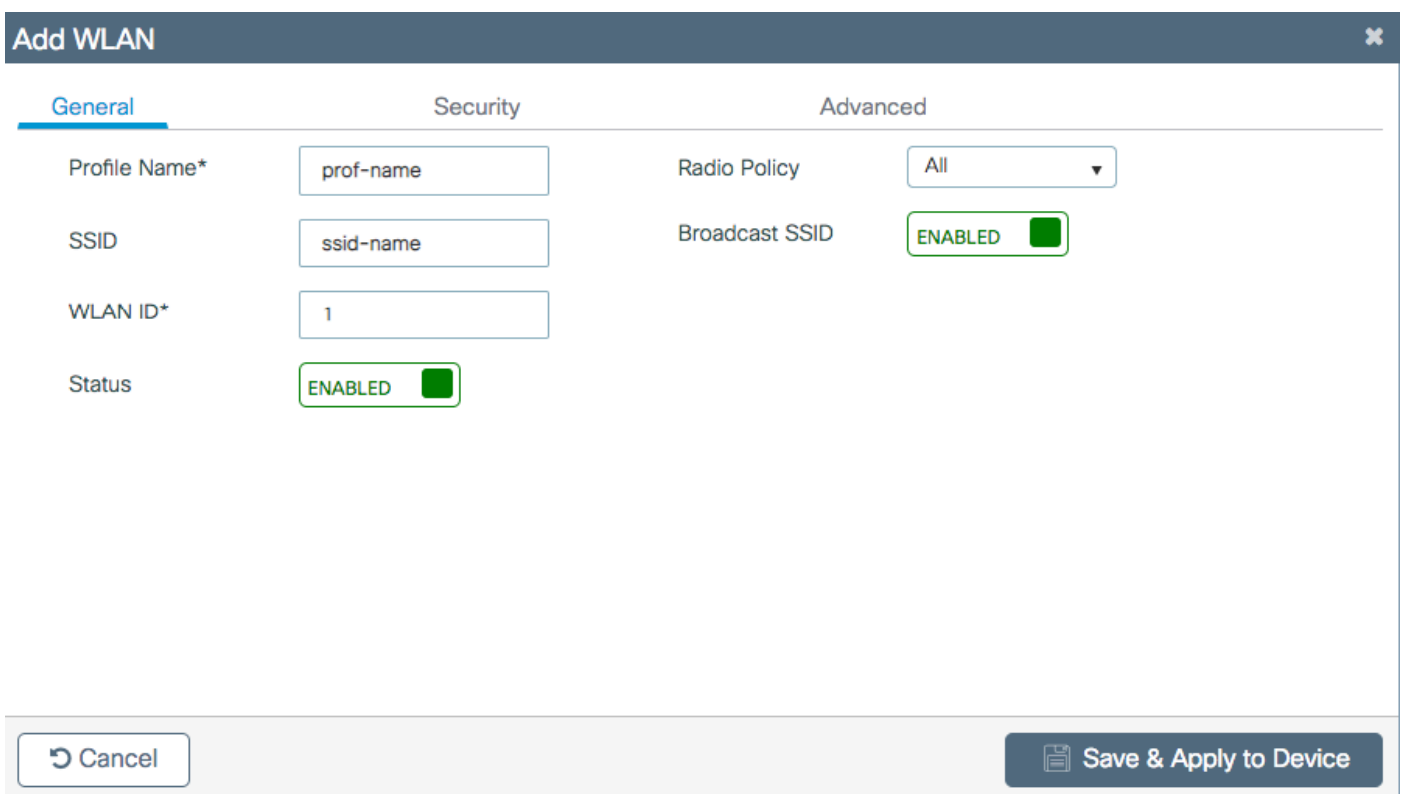
WLANプロファイルの設定

GUI :

ステップ 1 : WLANを作成します。[Configuration] > [Wireless] > [WLANs] > [+ Add] に移動し、必要に応じてネットワークを設定します。



ステップ 2 : WLAN情報を入力します

The image shows a screenshot of the 'Add WLAN' configuration form. The form has a dark header with the title 'Add WLAN' and a close button. Below the header are three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is selected and shows four fields: 'Profile Name*' with the value 'prof-name', 'SSID' with the value 'ssid-name', 'WLAN ID*' with the value '1', and 'Status' which is a toggle switch labeled 'ENABLED'. The 'Security' and 'Advanced' tabs are also visible. The 'Advanced' tab shows 'Radio Policy' set to 'All' and 'Broadcast SSID' which is a toggle switch labeled 'ENABLED'. At the bottom of the form are two buttons: 'Cancel' and 'Save & Apply to Device'.

ステップ 3：次に移動します。[Security] タブをクリックし、必要なセキュリティ方式を選択します。この例では、WPA2 + 802.1xです。

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. The 'Layer2' sub-tab is active. A red box highlights the 'Layer 2 Security Mode' dropdown menu, which is set to 'WPA + WPA2'. Other visible settings include 'MAC Filtering' (unchecked), 'Protected Management Frame' (disabled), 'PMF' (Disabled), 'WPA Parameters' (disabled), and 'WPA Policy' (unchecked). On the right side, 'Fast Transition' is set to 'Adaptive Enab...', 'Over the DS' is checked, and 'Reassociation Timeout' is set to 20. At the bottom, there are 'Cancel' and 'Save & Apply to Device' buttons.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected and the 'AAA' sub-tab active. The 'PMF' dropdown is set to 'Disabled'. The 'WPA Parameters' section is expanded. Under 'WPA Policy', 'WPA2 Policy' is checked. Under 'WPA2 Encryption', 'AES(CCMP128)' is checked, while 'CCMP256', 'GCMP128', and 'GCMP256' are unchecked. The 'Auth Key Mgmt' dropdown is set to '802.1x'. At the bottom, there are 'Cancel' and 'Save & Apply to Device' buttons. A red arrow on the right side of the window points downwards.

ステップ 4：Security > AAA タブで、[AAA Configuration on 9800 WLC] セクションのステップ3で作成した認証方式を選択します。

The screenshot shows the 'Add WLAN' configuration interface. It has three main tabs: 'General', 'Security', and 'Advanced'. Under 'Security', there are sub-tabs for 'Layer2', 'Layer3', and 'AAA'. The 'AAA' sub-tab is currently selected. In the 'Authentication List' field, a dropdown menu is open, showing 'list-name'. Below this, there is a checkbox for 'Local EAP Authentication' which is not checked. At the bottom right, there is a 'Save & Apply to Device' button.

CLI :

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```

ポリシープロファイルの設定

ポリシープロファイル内では、他の設定(アクセスコントロールリスト(ACL)、Quality of Service(QoS)、モビリティアンカー、タイマーなど)の中から、クライアントに割り当てるVLANを決定できます。

デフォルトのポリシープロファイルを使用することも、新しいプロファイルを作成することもできます。

GUI :

[Configuration] > [Tags & Profiles] > [Policy Profile] に移動し、**default-policy-profile**を設定するか、新しいプロファイルを作成します。

プロフィールを有効にします。

また、アクセスポイント(AP)がローカルモードの場合は、ポリシープロフィールで[Central Switching] と[Central Authentication] が有効になっていることを確認します。

[Access Policies] タブで、クライアントを割り当てる必要があるVLANを選択します。

Edit Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

VLAN2602



Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select



IPv6 ACL

Search or Select



URL Filters

Pre Auth

Search or Select



Post Auth

Search or Select



ISEがVLAN割り当てなどのAccess-Acceptで属性を返す予定の場合は、 **Advanced** tab:

✕
Edit Policy Profile

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

Policy Name

Fabric Profile

Umbrella Parameter Map

mDNS Service Policy [Clear](#)

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

5 GHz Policy

CLI :

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

ポリシータグの設定

ポリシータグは、SSIDとポリシープロファイルをリンクするために使用されます。新しいポリシータグを作成するか、default-policy タグを使用します。

注:default-policy-tagは、WLAN IDが1 ~ 16のSSIDを自動的にdefault-policy-profileにマッピングします。変更も削除もできません。ID 17以上のWLANがある場合、default-policy-tagは使用できません。

GUI :

移動先 **Configuation > Tags & Profiles > Tags > Policy** 必要に応じて新しいエントリを追加します。

Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Troubleshooting

Manage Tags

Policy Site RF AP

+ Add **✕ Delete**

Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

1 10 items per page

WLAN プロファイルを目的のポリシープロファイルにリンクします。

Add Policy Tag

Name* PolicyTagName

Description Enter Description

+ Add **✕ Delete**

WLAN Profile	Policy Profile

0 10 items per page No items to display

Cancel Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◁ 0 ▷ ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile*
Policy Profile*

✕
✓

↶ Cancel
Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile

◀ ◁ 1 ▷ ▶ 10 items per page 1 - 1 of 1 items

↶ Cancel
Save & Apply to Device

CLI :

```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

ポリシータグの割り当て

必要な AP にポリシータグを割り当てます。

GUI :

1つのAPにタグを割り当てるには、 Configuration > Wireless > Access Points > AP Name > General Tags, 関連するポリシータグを割り当て、 Update & Apply to Device.

Edit AP

General Interfaces High Availability Inventory Advanced

General

AP Name* AP3802-02-WS

Location* default location

Base Radio MAC 00:42:68:c6:41:20

Ethernet MAC 00:42:68:a0:d0:22

Admin Status Enabled

AP Mode Local

Operation Status Registered

Fabric Status Disabled

Tags

Policy default-policy-tag

Site default-site-tag

RF default-rf-tag

Version

Primary Software Version 10.0.200.50

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 1.0.0

IOS Version 10.0.200.02

Mini IOS Version 0.0.0.0

IP Config

IP Address 172.16.0.207

Static IP

Time Statistics

Up Time 9 days 1 hrs 17 mins 24 secs

Controller Associated Time 0 days 3 hrs 26 mins 41 secs

Controller Association Latency 8 days 21 hrs 50 mins 33 secs

Cancel Update & Apply to Device

注:APのポリシータグを変更すると、9800 WLCへの関連付けが解除され、数分後に元に戻ることに注意してください。

複数のAPに同じポリシータグを割り当てるには、次のURLに移動します。 Configuration > Wireless Setup > Advanced > Start Now > Apply.

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。