

# CBWネットワークにおけるRLANを使用したポート設定

## 目的

この記事の目的は、リモートローカルエリアネットワーク(RLAN)ネットワークを作成し、Cisco Business Wireless(CBW)プライマリアクセスポイント(AP)上でポートとアクセスポイントグループを割り当てることです。

## 該当するデバイス|ソフトウェアバージョン

- 145AC ([データシート](#)) | 10.4.1.0 ([最新版をダウンロード](#))
- 240AC ([データシート](#)) | 10.4.1.0 ([最新ダウンロード](#))

## はじめに

CBW APは802.11 a/b/g/n/ac(Wave 2)ベースで、内部アンテナを備えています。これらのAPは、最新の802.11ac Wave 2規格をサポートしており、より高いパフォーマンス、より優れたアクセス、より高密度なネットワークを実現します。

この記事で説明する145ACおよび240AC APは、従来のネットワークまたはメッシュネットワークで使用できます。この記事では、従来のワイヤレスネットワーク用の機器を使用します。

メッシュネットワークの基本を学習するには、『[シスコビジネス：ワイヤレスメッシュネットワークへようこそ](#)』をご覧ください。

メッシュネットワークでポート設定を行う場合は、『[メッシュモードでのCisco Business Wireless Access Point\(WAP\)のイーサネットポートの設定](#)』を参照してください。

従来のワイヤレスネットワークでは、プライマリAPを使用して有線クライアントを認証するためにRLANが使用されます。有線クライアントがプライマリAPに正常に参加すると、LANポートはトラフィックを中央またはローカルのスイッチングモード間で切り替えます。有線クライアントからのトラフィックは、ワイヤレスクライアントトラフィックとして扱われます。

RLANは、有線クライアントを認証するために認証要求を送信します。RLANでの有線クライアントの認証は、中央で認証されたワイヤレスクライアントと同様です。

仮想ローカルエリアネットワーク(VLAN)が1つだけ必要な場合、RLANを設定する必要はありません。デフォルトでは、1つのRLANがネイティブVLAN 1のAPに割り当てられます。オープンセキュリティがあり、デフォルトではすべてのポートがこのRLANに割り当てられています。

使用される用語に慣れていない場合は、「[シスコビジネス：新しい用語の用語集](#)」を参照してください。

RLANは、メッシュネットワークでは動作しません。デフォルトではメッシュは有効になっていないため、以前にAPをメッシュモードで実行していた場合を除き、実行するように設定されています。

## 設定手順

### 初級ヘルプ

この切り替えられたセクションでは、初心者向けのヒントを紹介します。

### ログイン

プライマリAPのWebユーザインターフェイス(UI)にログインします。これを行うには、Webブラウザを開き、<https://ciscobusiness.cisco>と入力します。続行する前に警告が表示される場合があります。クレデンシャルを入力します。Webブラウザに[https://\[ipaddress\]](https://[ipaddress]) (プライマリAPの) と入力して、プライマリAPにアクセスすることもできます。

### ツールヒント

ユーザインターフェイスのフィールドに関する質問がある場合は、次のようなツールヒントを確認してください。



## メインメニューの展開アイコンを見つけられない

画面の左側のメニューに移動します。メニューボタンが表示されない場合は、このアイコンをクリックしてサイドバーメニューを開きます。



## シスコビジネスアプリケーション

これらのデバイスには、一部の管理機能をWebユーザインターフェイスと共有するコンパニオンアプリケーションがあります。Webユーザインターフェイスのすべての機能がアプリで使用できるわけではありません。

[iOSアプリのダウンロード](#) [Androidアプリのダウンロード](#)

よく寄せられる質問 (FAQ)

まだ未回答の質問がある場合は、よく寄せられる質問(FAQ)のドキュメントを確認してください。  
。 [FAQ](#)

## 手順 1

アクセスポイントの電源が入っていない場合は、電源を入れます。インジケータライトのステータスを確認します。LEDライトが緑色に点滅したら、次の手順に進みます。

アクセスポイントの起動には、約8 ~ 10分かかります。LEDは複数のパターンで緑色に点滅し、緑色、赤色、およびオレンジ色の間で急速に交互に点滅した後、再び緑色に変わります。LEDの色の輝度と色合いには多少の違いがある場合があります。

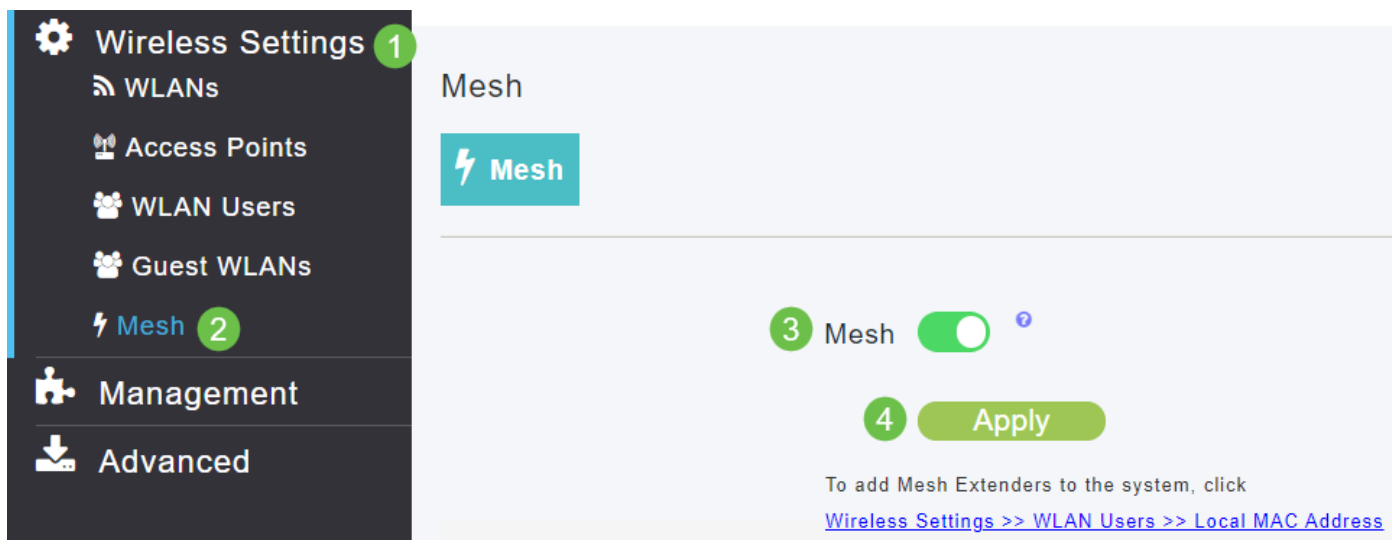
## 手順 2

プライマリAPのWebユーザインターフェイス(UI)にログインします。Webブラウザを開き、「<https://ciscobusiness.cisco>」と入力します。続行する前に警告が表示されることがあります。認証情報を入力してください。

プライマリAPのIPアドレスをWebブラウザに入力してアクセスすることもできます。

## 手順 3

RLANが機能するためにAPをメッシュモードにすることはできません。メッシュモードをオフにするには、Wireless Settings > Meshの順に選択します。メッシュをオフにする場合に選択します。APが新規の場合、またはメッシュモードがオンになっていないことが判明している場合は、[ステップ7](#)に進むことができます。



The screenshot displays the Cisco Business Manager interface. On the left, a dark sidebar contains a menu with 'Wireless Settings' (1) and 'Mesh' (2) highlighted. The main content area is titled 'Mesh' and features a green 'Mesh' button with a lightning bolt icon. Below this, a 'Mesh' toggle switch (3) is turned on. A green 'Apply' button (4) is positioned below the toggle. At the bottom of the page, a note reads: 'To add Mesh Extenders to the system, click [Wireless Settings >> WLAN Users >> Local MAC Address](#)'.

## 手順 4

Yesをクリックして、メッシュモードをオフにすることを確認します。

## Apply mesh configuration

By disabling the Mesh, all the mesh Extenders will be disconnected from this network and wired APs will rejoin after few minutes. Are you sure you want to continue?

Yes

No

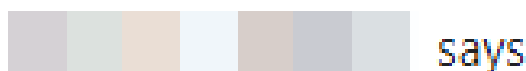
### 手順 5

Web UI画面の右上のパネルにあるSave iconをクリックして、設定を必ず保存してください。



### 手順 6

OKをクリックして、保存を確認します。APがリブートします。この処理には8 ~ 10分かかります。



Are you sure you want to save configuration to flash so that on a reboot the AP retains the configuration?

OK

Cancel

### ステップ7

RLANは、Wireless Settings > WLANsの順に選択して作成できます。次に、Add new WLAN/RLANを選択します。

Monitoring

Wireless Settings

WLANs

Access Points

WLAN Users

Guest WLANs

Mesh

Management

Advanced

Cisco Business Wireless

WLANs

Active WLANs 1

Active RLANs 1

Add new WLAN/RLAN

Action	Active	Type	Name	SSID	Security Policy	Radio Policy	
	Enabled	WLAN	EZ1K	EZ1K	Personal(WPA2)	ALL	
	Enabled	RLAN	DEFAULT_RLAN	DEFAULT_RLAN	Open	N/A	

## 手順 8

RLANを選択します。プロファイルの名前を作成します。

Add new WLAN/RLAN

General RLAN Security VLAN & Firewall Traffic Shaping

Network ID 3

Type RLAN

Profile Name \* RLAN2

Enable

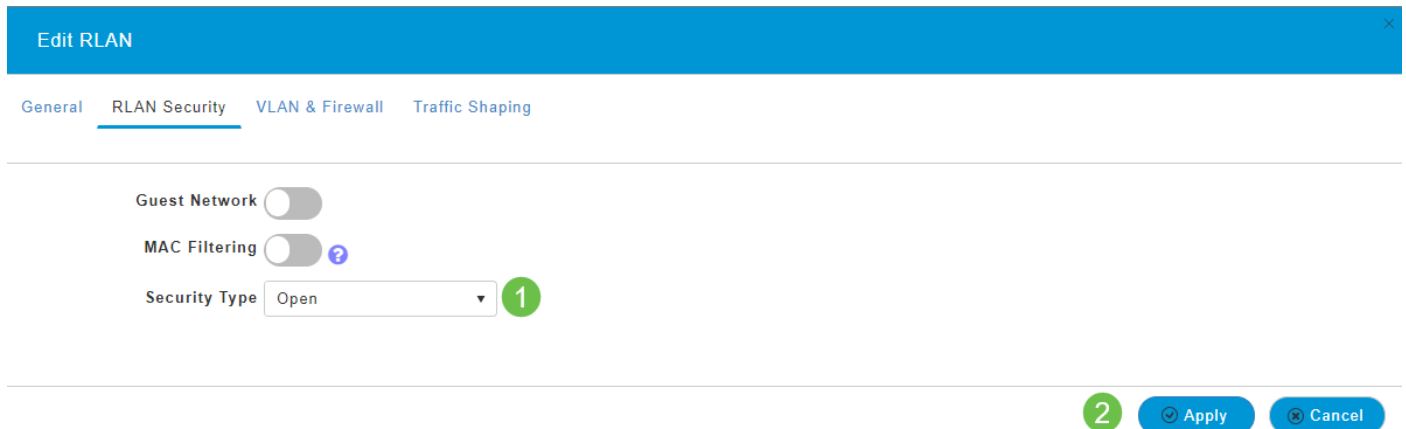
Apply Cancel

ステップ9 ( オープンセキュリティの使用 )

RLAN Securityタブの下にある手順を実行します。Security Typeで、Openまたは802.1Xを選択できます。

この例では、Security Typeはデフォルトのままになっています。

[APPLY] をクリックします。これにより、このオープンセキュリティRLANが自動的にアクティブになります。ステップ 11 に進みます。



Edit RLAN

General RLAN Security VLAN & Firewall Traffic Shaping

Guest Network

MAC Filtering  ?

Security Type Open **1**

**2** Apply Cancel

## ステップ10a ( 802.1Xセキュリティの使用 )

外部RADIUSを設定するには、Expert ViewのRADIUSでAdmin AccountsにRADIUS Serverを設定しておく必要があります。Web UIの右上のメニューにある矢印アイコンをクリックして、エキスパートビューに切り替えます。RADIUSサーバの設定の詳細については、[RADIUS](#)



# Switch to Expert View

## ステップ10b ( 802.1Xセキュリティの使用 )

セキュリティタイプとして802.1Xを選択した場合は、さらに多くのオプションを選択する必要があります。

あります。次の項目を選択する必要があります。

- ホストモード:シングルホストまたはマルチホスト
- 認証サーバ:外部RADIUSまたはAP
- MABモード : EnabledまたはDisabled。MACアドレスを追加するには、次の手順の指示に従います。

### Add new WLAN/RLAN

General RLAN Security VLAN & Firewall Traffic Shaping

Guest Network

MAC Filtering  ?

Security Type 802.1X ▼

Host Mode Single Host ▼ **1**

Authentication Server External Radius ▼ ? **2**

No RADIUS Server is configured for Authentication and Accounting. RADIUS Server can be configured from 'Admin Accounts > RADIUS'(Expert view)

MAB Mode

RADIUS Server

Add RADIUS Authentication Server **3**

State	Server IP Address	Port
-------	-------------------	------

## 手順 11 ( オプション )

MAC認証バイパス(MAB)モードは、WLANユーザの下にMACアドレスが表示されている場合に、デバイスを認証する必要がないことを意味します。リストされているMACアドレスは、認証をバイパスして、ネットワークへの自動アクセスを許可したり、自動的に拒否したりできます。これは、IP電話がスイッチのPoEポートに接続されている場合に役立ちます。

各MACアドレスには、次の2つの方法のいずれかでラベルを付けることができます。

1. Allowlisted : デバイスは自動的にアクセスを受け取ります。
2. Blocklisted : デバイスは自動的にアクセスを拒否されます。

The screenshot shows the Cisco Business Wireless 145AC Access Point configuration page. The left sidebar contains navigation options: Monitoring, Wireless Settings (1), WLANs, Access Points, WLAN Users (2), Guest WLANs, Mesh, Management, and Advanced. The main content area is titled 'WLAN Users' and shows a 'Users' count of 1. Below this, there are tabs for 'WLAN Users' and 'Local MAC Addresses' (3). A search bar and a table are visible. The table has columns for Action, MAC Address, Type, Profile Name, and Description. It lists three entries, all of type 'Allowlist'.

Action	MAC Address	Type	Profile Name	Description
	a4: : : 20	Allowlist	Any WLAN/RLAN	CBW145AC-0b20
	4c: : : 68	Allowlist	Any WLAN/RLAN	CBW141ACM-7468
	4c: : : 1	Allowlist	Any WLAN/RLAN	CBW140AC-cba1

## 手順 12

VLAN & Firewallタブで、Use VLAN Taggingを選択し、VLAN ID番号を選択できます。

The screenshot shows the 'VLAN & Firewall' configuration page. The top navigation bar includes 'General', 'RLAN Security', 'VLAN & Firewall', and 'Traffic Shaping'. The main content area has four settings:

- Client IP Management: External DHCP Server
- Use VLAN Tagging: Yes (1)
- VLAN ID \*: 5 (2)
- Enable Firewall: No

At the bottom, there is a confirmation message: 'VLAN and Firewall configuration apply to all WLANs and RLANs configured with same VLAN'. To the right of the message are 'Apply' and 'Cancel' buttons.

## 手順 13 ( オプション )

特定のIPアドレスやVLANへのアクセスを許可または拒否できるアクセスコントロールリスト (ACL)を設定する場合は、Enable Firewallを選択します。これは、誰かがネットワークポートデバイスに接続してネットワークに接続する場合に使用されます。

Client IP Management External DHCP Server ▼

Use VLAN Tagging Yes ▼

VLAN ID \* 5 ▼

Enable Firewall Yes ▼

1

#### WLAN Post-auth ACL

ACL Name(IPv4) None ▼

ACL Name(IPv6) None ▼

2

#### VLAN ACL

ACL Name(IPv4) None ▼

ACL Direction Ingress ▼

### 手順 14 ( オプション )

Traffic Shapingタブで、Application Visibility Controlをイネーブルにすることで、トラフィックシ

エーピングを設定できます。これにより、トラフィックのプライオリティが設定されます。

General RLAN Security VLAN & Firewall Traffic Shaping

Application Visibility Control

Enabled

1

AVC Profile

RLAN2

Add Rule

2

Action	S.L No.	Application	Action
<			>
<			>

Apply

Cancel

## ステップ 15 ( オプション )

Schedulingタブで、スケジュールを選択できます。ポートがネットワークに接続できる時間が設定されます。

**Add new WLAN/RLAN**

General RLAN Security VLAN & Firewall Traffic Shaping Scheduling

Schedule WLAN: No Schedule

When 'No Schedule' is selected, all the below scheduling information would be cleared.

Apply to all weekdays:

Day	Availability	From	To
Monday	<input type="checkbox"/>	00:00	23:59
Tuesday	<input type="checkbox"/>	00:00	23:59
Wednesday	<input type="checkbox"/>	00:00	23:59
Thursday	<input type="checkbox"/>	00:00	23:59
Friday	<input type="checkbox"/>	00:00	23:59
Saturday	<input type="checkbox"/>	00:00	23:59
Sunday	<input type="checkbox"/>	00:00	23:59

## 手順 16 ( オプション )

RLANが作成されたので、Wireless Settings > Access Point Groupsの順に移動します。ここでは、グループを追加または編集できます。この画面を表示するには、ステップ10aで選択した[エキスパートビュー](#)である必要があります。

Wireless Settings 1

- WLANs
- Access Points
- Access Points Groups 2
- WLAN Users
- Guest WLANs
- Mesh

Management

Services

Advanced

Access Points Groups

Access Points Groups 1

Add new group Refresh

Action	AP Group name
<input type="checkbox"/> x	Warehouse
<input type="checkbox"/>	default-group

10 items

Add new group

General WLANs Access Points RF Profile Ports

3 AP Group name Warehouse

AP Group description

Apply Cancel

## 手順 17

Portsタブでは、APのポートを特定のリモートLANに割り当てることができます。

Port	Status	PoE	Remote LAN
LAN 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	DEFAULT_RLAN
LAN 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RLAN
LAN 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	DEFAULT_RLAN
LAN 4	<input type="checkbox"/>	<input type="checkbox"/>	None

Apply Cancel

## 手順 18

Access Pointsタブで、特定のアクセスポイントをそのアクセスポイントグループに割り当てる必要があります。[APPLY] をクリックします。

Edit Warehouse

General WLANs Access Points RF Profile Ports

Search Refresh

APs in "Warehouse" group AP Group All

AP Name	MAC Address
No items to display	

AP Name	AP Group name
AP4C8C.48C0.74B8	default-group
<input checked="" type="checkbox"/> APA453.0E1E.2338	default-group

1

2

Apply Cancel

## 手順 19

Yesを選択して確定します。

Confirmation

Selected APs will be moved to Warehouse group. Clients connected to these APs may experience network disruption. Are you sure you want to continue?

Yes No

## 手順 20

Web UI画面の右上のパネルにあるSave iconをクリックして、設定を必ず保存してください。



## ステップ 21

OKをクリックして、保存を確認します。APがリブートします。この処理には8 ~ 10分かかります。

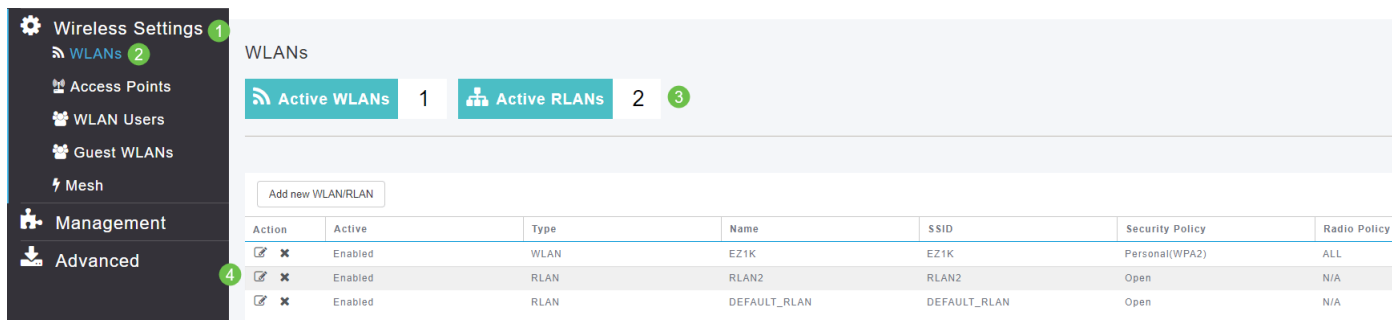


Are you sure you want to save configuration to flash so that on a reboot the AP retains the configuration?



## RLANの表示

作成したRLANを表示するには、Wireless Settings > WLANsの順に選択します。アクティブRLANの数が2に増え、新しいRLANがリストされます。



Action	Active	Type	Name	SSID	Security Policy	Radio Policy
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	WLAN	EZ1K	EZ1K	Personal(WPA2)	ALL
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	RLAN	RLAN2	RLAN2	Open	N/A
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	RLAN	DEFAULT_RLAN	DEFAULT_RLAN	Open	N/A

## RLANの編集

RLANのセットアップの最後にApplyをクリックすると、RLANが自動的にアクティブ化されます。RLANを無効にしたり、その他の変更を行う必要がある場合は、次の簡単な手順に従ってください。

### 手順 1

Wireless Settings > WLANsの順に選択します。編集アイコンをクリックします。

Wireless Settings 1

WLANs 2

Access Points

WLAN Users

Guest WLANs

Mesh

Management

Advanced 3

WLANs

Active WLANs 1 Active RLANs 2

Add new WLAN/RLAN

Action	Active	Type	Name	SSID	Security Policy	Radio Policy
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	WLAN	EZ1K	EZ1K	Personal(WPA2)	ALL
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	RLAN	RLAN2	RLAN2	Open	N/A
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	RLAN	DEFAULT_RLAN	DEFAULT_RLAN	Open	N/A

## 手順 2

RLANを編集するとネットワークが一時的に中断されることを通知するポップアップが表示されます。Yesをクリックして、続行することを確認します。

Edit RLAN

RLAN is in enable state. Editing the RLAN configuration will disrupt the network momentarily. Do you want to continue.?

Yes No

## ステップ3 (有効/無効)

Edit WLAN/RLANウィンドウのGeneralの下で、EnabledまたはDisabledを選択して、RLANを有効または無効にします。[APPLY] をクリックします。

## Edit RLAN



General

RLAN Security

VLAN & Firewall

Traffic Shaping

Network ID

3

Type

RLAN

Profile Name \*

RLAN2

Enable



2

Apply

Cancel

### ステップ4 ( その他の設定の編集 )

設定を変更する必要がある場合は、RLAN Security、VLAN & Firewall、またはTraffic Shapingタブに移動します。変更が完了したら、Applyをクリックします。

## Edit RLAN



General

RLAN Security

VLAN & Firewall

Traffic Shaping

1

Guest Network



MAC Filtering



Security Type

Open

2

Apply

Cancel

### 手順 5

Web UI画面の右上のパネルにあるSave iconをクリックして、設定を必ず保存してください。



## 結論

これで、CBWネットワーク上にRLANが作成されました。お客様のニーズに合わせて自由に追加できます。

[よく寄せられる質問Radius](#) [ファームウェアアップグレードRLAN](#) [アプリケーションプロファイリングクライアントプロファイリング](#) [プライマリAPツール傘](#) [WLANユーザーログイン](#) [トラフィックシェーピングの不正](#) [干渉設定管理](#) [ポート設定メッシュモード](#) [CBWへようこそメッシュネットワーク](#) [電子メール認証とRADIUSアカウント](#) [ングを使用したゲストネットワークCBWとDraytekルータの使用に関するトラブルシューティング](#)

## 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。