



CTC テクノロジー株式会社

# 目次

動作環境.....

# Windows 向けセットアップ.....

Cisco AnyConnect Secure Mobility Client のインストール	4
接続確認	7

### トラブル時の対応.....10

キャッシュのクリア	10
IPv6 の無効化	11
よくあるご質問	

3

.4

## 動作環境

Cisco AnyConnect の動作環境として、下記 OS を推奨しています。

- Windows 10 x64 (64-bit)
- Windows 11 x64 (64-bit)

社内ネットワークから接続する場合、社内のセキュリティポリシーにより接続拒否される 場合があります。その際は、社内セキュリティ管理者にお問い合わせいただくか、ご自宅等 の社内ネットワーク以外のインターネット接続環境をご用意ください。

# Windows 向けセットアップ

Cisco AnyConnect Secure Mobility Client のインストール

① Google Chrome などの Web ブラウザから、下記 URL ヘアクセスします。

https://122.220.28.45/ctct

表示された画面で下記のユーザー名とパス ワードを入力し、ログインしてください。

> USERNAME : ctct PASSWORD : Cisc0As@

Login
Please enter your username and password.
USERNAME: ctct PASSWORD: ·······
Login

(注)正しいURLを入力しても画面が表示されない場合や、正しいパスワードを入力しても「Login failed.」と表示される場合は、ブラウザのキャッシュをクリアしてください。キャッシュクリア の方法は、本ドキュメント後半のトラブル時の対応をご確認ください。

正しくログインできると、ダウンロード画面が表示されます。

ダウンロードボタンをクリックし、インストーラーをダウンロードします。
 ダウンロードが完了したら、ファイルを実行してください。

Download & Install
Download Cisco AnyConnect Secure Mobility Client and install it on your computer.
Download for Windows
Instructions

③ インストーラーが起動し、AnyConnect Secure Mobility Client のセットアップが開始し ます。



「Next」をクリックします。





上側の「I accept the terms in the License Agreement」のラジオボタンを選択し、 「Next」をクリックします。

「Install」をクリックします。



ユーザーアカウント制御の以下の画面が表示 された場合は、「**はい**」をクリックします。



インストールが完了するまでしばらく待ちま す。インストールが完了すると以下の画面が 表示されるので、「**Finish**」をクリックします。



Windows のスタートメニューを開いて、 「Cisco」 > 「Cisco AnyConnect Secure Mobility Client」をクリックします。



この画面が表示されれば、インストール成功 です。

#### 接続確認

① SSL-VPN を確立して、リモートラボ機材へアクセスの確認を行います。



Cisco AnyConnect Secure Mobility Client の画面で、「**122.220.28.45/ctct**」 と入力し「**Connect**」をクリックします。

	Please ente	r your username and password.
-	Username:	ctct
	Password:	*******

ユーザー名とパスワードを下記のとお り入力し、「**OK**」をクリックします。

> USERNAME : ctct PASSWORD : Cisc0As@

60	VPN:			
	Connected to 122.220.28.4	15/ctct.		
_	122,220,28,45/ctct	×	Disconnect	

鍵のイラストに緑のチェックボックス が追加され、「Connected」と表示されれ ば SSL-VPN 確率成功です。

 ② コマンドプロンプトを起動して、疎通確認を行います。
 Windows 10 であれば、「スタートメニュー > Windows システム ツール > コマンド プロンプト」の手順で起動できます。



コマンドプロンプトの画面で「ping 192.168.142.128」と入力し、**192.168.142.128** か **らの応答**」が表示されることを確認します。

■ 管理者: コマンド プロンプト	0	23
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.		* H
C:¥>ping 192.168.142.128		
192.168.142.128 に ping を送信しています 32 バイトのデータ: 192.168.142.128 からの応答: バイト数 =32 時間 =303ms TTL=254 192.168.142.128 からの応答: バイト数 =32 時間 =489ms TTL=254 192.168.142.128 からの応答: バイト数 =32 時間 =73ms TTL=254 192.168.142.128 からの応答: バイト数 =32 時間 =153ms TTL=254		
192.168.142.128 の ping 統計: パケット数:送信 = 4、受信 = 4、損失 = 0 (0% の損失)、 ラウンド トリップの概算時間 (ミリ秒): 最小 = 73ms、最大 = 489ms、平均 = 254ms C:¥>		

🕥 Cisco AnyO	Connect Secure Mobility Client			×
r?	VPN: Connected to 122.220.28.45/ctct.	_		
	122.220.28.45/ctct		Disconnect	
00:26:46		0	IP∖	/4

確 認 が で き た ら 、 AnyConnect Secure Mobility Client の 「**Disconnect**」をクリック して、SSL-VPN 接続を切断してください。

#### 研修当日の接続方法

Windows のスタートメニューを開いて、「Cisco」>「Cisco AnyConnect Secure Mobility Client」とクリックし、Cisco AnyConnect Secure Mobility Client を起動します。

Cisco AnyConnect Secure Mobility Client の以下の画面において、研修当日にインストラク ターより案内されたアドレス、ユーザー名、パスワードを入力して SSL-VPN 接続を行いま す。

Scisco AnyConnect Secure Mobility Client	- 🗆	× 🚳 (	Cisco AnyConnect   122.220.28.45	
Ready to connect.	<ul> <li>Connect</li> </ul>	-	Please enter your username a Username: Password:	nd password.
<b>\$</b> ()		uludu. cisco	0	K Cancel

(注)研修では、演習機材に接続するための専用のアドレス、ユーザー名、パスワードを使用します。接続確認で入力したアドレス「122.220.28.45/ctct」、Username「ctct」、Password「CiscOAs@」は使用しないので、ご注意ください。

続いて、リモートデスクトップ接続を行います。

Windows のスタートメニューを開いて、「Windwos アクセサリ」>「リモートデスクトップ接続」をクリックし、インストラクターから案内された情報を入力します。

以降の操作は、インストラクターの指示に従ってください。

•	■ ステップ記録ツール	100 リモート デスクトップ接続 – 🗌 X
8	<i>ब्यू</i>	▶ リモート デスクトップ
Ľ		後 接続
	秋季 文字コード表     ホー     ホー	
~	🌄 リモート デスクトップ接続	コンビュージー(C) [[2]: CONPUELIADIKANICON
£03	▶ ワードパッド	コンピューター名フィールドが空白です。
Φ	Windows 簡単操作	リモートコンピュージーの完全な名削を入力してくたさい。
-	🖬 🧕 کَر	★プションの表示(O)     接続(N)     へルブ(H)

## トラブル時の対応

#### キャッシュのクリア

正しい URL を入力してもページが表示されない場合や、正しいパスワードを入力しても 「Login failed.」と表示される場合は、ブラウザのキャッシュをクリアしてください。

#### Google Chrome の場合

ブラウザ右上の「!」をクリックし、設定を開きます。

「プライバシーとセキュリティ」の「閲覧履歴データの削 除」をクリックし、「**Cookie と他のサイトデータ**」と 「**キャッシュされた画像とファイル**」のチェックを入れ、 「**データを削除**」をクリックしてください。

				☆	*	•	
	新しいタブ					Ctrl+T	
	新しいウィ	ンドウ				Ctrl+N	
	新しいシー	クレット	ウィンド	ゥ	Ctrl+	Shift+N	
	履歴						Þ
	ダウンロート	-				Ctrl+J	
	ブックマーク	7					۲
	ズーム		-	110%	+	53	
	印刷					Ctrl+P	
	検索					Ctrl+F	
	その他のツ	-JL					۲
	編集	切り	取り	3Ľ-	-	貼り付け	ł
	設定						
	ヘルプ						Þ
	終了						
<u>ا</u>	組織によっ	て管理	อ่กระ	ます			

プライ	パシーとセキュリティ	
Î	閲覧履歴データの削除 閲覧履歴、Cookie、キャッシュなどを削除します	•
۵	Cookie と他のサイトデータ シークレット モードでサードパーティの Cookie がブロックされています	•

閲覧履歴データの削除			
	基本設定	詳細設定	
期間	過去 24 時間		
	<b>閲覧履歴</b> 検索ボックスの履歴とオートコンス	プリート データを削除します	
<b>~</b>	Cookie と他のサイトデータ ほとんどのサイトからログアウトし	<b>/</b> ます。	
✓	キャッシュされた画像とファイル 最大で 39.3 MB を解放します。サイトによっては、次回アクセスする際に 読み込みに時間がかかる可能性があります。		
		キャンセルデータを削除	

#### IPv6 の無効化

一部の環境において、SSL-VPN 接続確立時に Web アクセスをはじめとしたインターネットの使用に問題が発生する可能性があります。

問題が発生した場合は、一時的に IPv6 接続を無効にします。

以下2つの手順のどちらかを実施して、ネットワーク接続を開きます。

- A) コントロールパネルを開き、次の手順でクリックします
   「ネットワークとインターネット」
   >「ネットワークと共有センター」
   > 左ペインの「アダプターの設定の変更」
- B) Windows の検索ボックスに「ncpa.cpl」と入力して Enter キーを押下します

ネットワーク接続を開いたら、インターネット接続に使用しているインターフェイスを右 クリックしてプロパティを開きます。 (イーサネットや Wi-Fi といった名称である場合が多いです)

プロパティが開いたら、「インターネット プロトコル バージョン 6(TCP/IPv6)」の項目の チェックを外して、OK ボタンをクリックします。

▶ ネットワーク接続	📮 1-サネットのプロパティ 🛛 🗙
← → ◇ ↑ 📴 > コントロール パネル > ネットワークとインターネット > ネットワーク接続	ネットワーク 共有
整理 ▼	接続の方法:
Cisco AnyConnect Secure Mobility Cisco AnyConnect Secure Mobility	Intel(R) 82574L Gigabit Network Connection
Client Connection 識別されていないネットワーク に tel(R) 82574L Gigabit Network C	構成(C) この接続は次の項目を使用します(O):
	✓ 望 QoS / (ケット スケジューラ     ▲       ✓ コンターネット プロトコル パージョン 4 (TCP/IPv4)     ▲       ▲ Microsoft Network Adapter Multiplexor Protocol     ▲       ✓ ▲ Microsoft IDP プロトコル パージョン 4 (TCP/IPv6)     ▲       ▲ Concert Tubeling Discovery Mapper I/O Driver     ▲       ▲ Link-Layer Topology Discovery Mapper I/O Driver     ✓
	<b>インストール(N)</b> 削除(U) プロパティ(R)
	説明 TCP/IP version 6。相互接続されたさまざまなネットワーク間の通信を提 供する、最新のインターネットプロトコルです。
	OK キャンセル

#### よくあるご質問

事前接続時、研修受講時によくあるご質問は下記をご確認ください。 解決されない場合はお問い合わせください。

Q. 接続確認をしたいのですが「https://122.220.28.45/ctct」に接続できません。

- Q. Cisco AnyConnect Secure Mobility Client (SSL-VPN クライアント)をインストールし ましたが、接続確認でエラーが発生します。
- A. 社内ネットワークからのアクセスの場合、御社内のネットワークセキュリティの制限で SSL-VPNの接続が出来ない可能性が考えられます。 その際はご自宅等のネットワークセキュリティの制限がないネットワークからご参加 いただくようご調整をお願い致します。
- Q. Cisco AnyConnect Secure Mobility Client (SSL-VPN クライアント) のインストールが できません。
- A. 業務用 PC からのご受講の場合、御社内のセキュリティポリシー上インストールができ ない場合や管理者用パスワードの入力が求められる場合があります。 その際は、個人所有の PC からご参加いただくようご調整をお願いいたします。

Q. 研修で使用する Cisco AnyConnect の接続先は、事前確認した接続先と違うのですか?

A. 事前確認で使用した Cisco AnyConnect の接続先は接続正常性の確認用途のため、研修 では使用しません。研修で使用する接続先は、研修当日に担当講師からお伝えします。

Cisco AnyConnect のインストールおよび接続確認(Windows 用)

2024年10月30日 Ver.9.0 発行元 CTC テクノロジー株式会社 〒102-0071 東京都千代田区富士見1-11-5 栗田九段ビル TEL: 0120-667230 FAX: 0120-667235 URL: http://www.school.ctc-g.co.jp/



●本書内に記載されている各製品名は、全て該当する所有者の商標または登録商標です。
 ●本書の無断複写および複製は著作権者の利益侵害になります。