

<目次>

0.	はじめに3
1.	ご利用フロー4
2.	インストール/アンインストールにあたっての注意事項5
3.	USBトークンドライバのインストール6
4.	VPNクライアント2のインストール-19
	VPNクライアント2のインストール -2 13
5.	V P Nクライアント2の初期設定17
6.	プロキシサーバーの設定21
7.	VPNの接続方法と切断方法25
8.	接続できない場合
9.	VPNクライアント2のアンインストール41
10.	USBトークンドライバのアンインストール44
11.	注意事項

0. はじめに

本マニュアルはセキュアネットワークサービスをご利用頂くにあたって必要となるク ライアントソフト(セキュアネットワーク VPN クライアント2)の設定について記述し ています。

 最新の VPN クライアントソフト、ドライバ及びマニュアルは随時更新されますので、 適時、ダウンロードして頂きますようお願い致します。閲覧には VPN クライアント によるセキュアネットワークセンターへの接続が必要です。 セキュアネットワーク インフォメーション サイト: http://www.info

○ VPN クライアント2 (Windows 11/10/8.1/8) の稼働条件

OS: Windows 11 (64bit)、10 x64 (64bit)、8.1 x86 (32bit)、Windows 8.1 x64(64bit) 注意: Windows 9x/ME/2000/XP/Vista/ServerOS には対応していません Windows 7/7 Starter Edition には対応していません Windows RT には対応していません アップグレードした OS には対応していません

CPU: Pentium クラス以上のプロセッサ Memory: 2GB 以上推奨 Hard Disk 空き容量: 100 MB 以上 その他: Microsoft インストーラー3.1 が利用可能であること

●おことわり

- ・ 本書の内容は断りなく変更することがあります。
- 本書および本書に記載されたソフトウェアの使用によって発生した損害およびその回復に要する費用に対し、当社は一切責任を負いません。
- ・ 本ソフトウェアを国外に持ち出したり、国外で利用したりすることによって発生した損害およびその回復に要する費用に対し、当社は一切責任を負いません。

1. ご利用フロー

1. 新規ご利用フロー



2. インストール/アンインストールにあたっての注意事項

(1) 他社 VPN ソフト(本ソフトの旧 Version も含む)との競合

本ソフトをインストールする端末に本ソフトの旧バージョンもしくは他社製の VPN ソフトがインストールされている場合、本ソフトをインストールする事で OS が起動しない、OS が強制終了される等の不具合がおきることがあります。PC 管理 者、レセコン業者、PC 購入元等にお問合せのうえ、問題がなければアンインストー ルした状態で本ソフトをインストールして下さい。

インストール済みVPNソフトの確認方法

コントロールパネルの「プログラムの追加と削除」でインストール済みのプログラム一覧及びスタートメニューのすべてのプログラムでVPNソフトの有無を確認します。

(2) ウイルス対策ソフトとの競合

ウイルス対策ソフトを利用されている場合はウイルス対策ソフトを一時的に無効 にして本ソフトのインストールをおこなって下さい。ウイルス対策ソフトが有効の ままインストールを行なうと、本ソフトのインストールが正常に行なえない事があ ります。本ソフトのインストールが完了した後、ウイルス対策ソフトの設定を有効 に戻すのを忘れないようにご注意願います。

(3) インストール/アンインストール作業の Windows 権限

VPN クライアントと USB トークンのドライバのインストール/アンインストー ルは Administrators 権限を持った Windows アカウントで行って下さい。

(4) ご利用される Windows アカウント名

セキュアネットワークサービスをご利用される Windows アカウント名が日本語 の場合、正常に動作しません。新しく英数字で Windows アカウント名を作成して 下さい。

(例) セキュアネットワークサービス…NG SecurenetworkService…OK

(5) 対応 USB トークン

青色 USB トークンは Windows 10/11 ではご利用いただけません。緑色 USB ト ークンに交換が必要です。詳細は購入元へお問い合わせ下さい。

3. USBトークンドライバのインストール

- CD-ROM を挿入すると自動的にブラウザが起動します。既に CD-ROM が入って いる場合は CD-ROM を入れ直します。(起動しない場合は CD-ROM 内の vpnclient2¥index.html ファイルをダブルクリックして下さい。)
- (2) 「2. USB トークンドライバのインストール」の "USB トークンドライバ(各 OS 共通)" をクリックします。
- (3)

	Secure Network Service
1	1. ドキュメント
1	シストールの前に下記のマニュアルをご一読ください。
	 ・ インストールガイド 3 ご利用マニュアル ³
2	2. USBトークンドライバのインストール
т	記のリンクよりインストールしてください。
-	 <u>USBトークンドライバ(各OS共通)</u>□
V	Vindows11/10/8.1/8用 以下のリンクをクリックしてインストールを行ってください。
	 インストーラ起動コ ※蓄告画面が出た場合は「実行」を選択してください。
	インストールできない場合
	ブラウザのセキュリティ領範により直接インストーラを起動できない可能性があるため、以下 の手順でインストーラを起動してください。
	ブラウザのセキュリティ機能により直接インストーラを起動できない可能性があるため、以下 の手順でインストーラを起動してください。 ②こりライブを避動してください。 ②こりテイブを避免して、耐ってくたさい。 ③ファイル「vpnclient_setup」をダブルクリックして実行してください。

(4) セキュリティ警告が表示された場合は、[保存]をクリックします。



(5) ユーザーアカウント制御が表示された場合は、[はい]をクリックします。



(6) "日本語"を選択し、[OK]をクリックします。

言語選択	×
12	インストールウィザードの言語をご選択くださ い。
	日本語
	OK ++>ZU

(7) インストーラが実行されますので[次へ]をクリックします。

骨 ePass2003 セットアップ	
	ePass2003 セットアップ ウィザードへようこそ
B	このウィザードは、ePass2000のインストールをガイドしていきます。 セットアップを開始する前に、他のすべてのアプリケーションを終了 することを推奨します。これによってセットアップがコンピュータを再 起動せずに、システム ファイルを更新することが出来るようになりま す。 続けるには DXへ] をクリックして下さい。
	次へ(N)> キャンセル

第8.0版

(8) [インストール]をクリックします。



(9) インストールが開始されます。

得 ePass2003 セットアップ	- D X
インストール ePass2003をインストールしています。しばらくお待ちください。	
ショートカットの作成:C¥ProgramData¥Microsoft¥Windows¥Start Menu¥Progra	ms¥EnterSafe¥ePass2008
Windows Installer	
< 戻る(B) 次へ	(N) > キャンセル

(10)[完了]をクリックします。



(11)以上で USB トークンドライバのインストールは終了です。 ※再起動は不要です。

4. VPNクライアント2のインストール-1

※インストーラがうまく起動しない場合は「4. VPNクライアント2のインストール-2」 を参照願います。

- 注意:Windows 9x/ME/2000/XP/Vista/ServerOS には対応していません。 Windows 7/7 Starter Edition、Windows RT には対応していません。 アップグレードした OS には対応していません。 全てのアプリケーションを終了してから実行して下さい。
 - CD-ROM を挿入すると自動的にブラウザが起動します。既に CD-ROM が入って いる場合は CD-ROM を入れ直します。(起動しない場合は CD-ROM 内の vpnclient2¥index.html ファイルをダブルクリックして下さい。)
 - (2) 「3.VPN クライアント2のインストール」の "<u>インストーラ起動</u>"をクリック します。

Secure Network Service
1. ドキュメント
インストールの前に下記のマニュアルをご一読ください。
 ・ インストールガイド™ ・ ご利用マニュアル™
2. USBトークンドライバのインストール
下記のリンクよりインストールしてください。
- <u>USBトークンドライバ(各OS共通)</u> □
3. VPNクライアント2(Ver.4.10.05095)のインストール
Windows11/10/8.1/8用
以下のリンクをクリックしてインストールを行ってください。
・ インストーラ起動コ
※普告画面が出た場合は「実行」を選択してください。
・インストールできない場合
ブラウザのセキュリティ機能により直接インストーラを起動できない可能性があるため、以下 の手順でインストーラを起動してください。
 エクスプローラを起動してください。 CDドライブを選択して、開いてください。
③ファイル「vpnclient_setup」をダブルクリックして実行してください。

(3) セキュリティの警告が表示された場合は、[実行]をクリックします。



(4) インストーラが実行されますので[次へ]をクリックします。



(5) "使用許諾契約書のすべての条項に同意します(A)"を選択し、[次へ]をクリックしま



(6) [インストール]をクリックします。

🖞 Cisco AnyConnect Secure Mobility Client セットアップ
インストール準備完了 セットアップウィザードはCisco AnyConnect Secure Mobility Clientインス
[インストール]をクリックしてインストールを開始してください。 インストールの設定を変更する場合は[戻る]をクリックしてください。[キャンセル]をクリックする と、セットアップを中止します。
Advanced Installer
〈戻る ⑧〉 【インストール() キャンセル

(7) ユーザーアカウント制御が表示された場合は、[はい]をクリックします。

-ב 😗	-ザー アカウント制	御
次の不明な発行元からのプログラムにこのコンピューターへの変更を許可しますか?		
	プログラム名: 発行元: ファイルの入手先	E:¥vpnclient2¥vpnclient¥vpnclient_setup.msi 不明 :: CD/DVD ドライブ
v 1	¥細を表示する(<u>D</u>)	はい(Y) りいえ(N) これらの通知を表示するタイミングを変更する

(8) インストールが開始されます。



(9) [完了]をクリックします。



(10) 以上で VPN クライアント2のインストールは終了です。

※再起動は不要です。

「5. VPNクライアント2の初期設定」の手順に進んでください。

4. VPNクライアント2のインストール-2

 CD-ROM を挿入すると自動的にブラウザが起動します。既に CD-ROM が入って いる場合は CD-ROM を入れ直します。(起動しない場合は CD-ROM 内の vpnclient2¥index.html ファイルをダブルクリックして下さい。)

Secure Network Service		
1. ドキュメント		
インストールの前に下記のマニュアルをご一読ください。		
・ <u>インストールガイド</u> ≊ ・ <u>ご利用マニュアル</u> ≊		
2. USBトークンドライバのインストール		
下記のリンクよりインストールしてください。		
- <u>USBトークンドライバ(各OS共通)</u> □		
3. VPNクライアント2(Ver.4.10.05095)のインストール		
Windows11/10/8.1/8用		
以下のリンクをクリックしてインストールを行ってください。 ・ インストーラ起動コ		
※警告画面が出た場合は「実行」を選択してください。		
・インストールできない場合		
ブラウザのセキュリティ機能により直接インストーラを起動できない可能性があるため、以下 の手順でインストーラを起動してください。		
 ①エクスブローラを起動してください。 ②CDドライブを選択して、聴いてください。 ③ファイル「vpnclient_setup」をダブルクリックして実行してください。 		

Windows エクスプローラから CD-ROM の入った CD/DVD ドライブをクリックします。



(3) [vpnclient_setup] をクリックします。

名前	更新日時	種類	サイズ
📙 image	2022/10/20 17:20	ファイル フォルダー	
vpnclient2	2022/10/20 17:20	ファイル フォルダー	
AUTORUN.INF	2015/10/06 15:23	セットアップ情報	1 KB
ディレクトリ構成 byt	2022/10/28 9:15	テキスト ドキュメント	1 KB
	2022/10/28 18:43	ショートカット	5 KB

(4) セキュリティの警告が表示された場合は、[実行]をクリックします。





(6) "使用許諾契約書のすべての条項に同意します(A)"を選択し、[次へ]をクリックしま





第8.0版

(7) [インストール]をクリックします。

🕼 Cisco AnyConnect Secure Mobility Client セットアップ	X
インストール準備完了 セットアップウィザードは Cisco AnyConnect Secure Mobility Clientインストー	2
【インストール】をクリックしてインストールを開始してください。 インストールの設定を変更する場合は【戻る】をクリックしてください。【キャンセル】をクリ・ と、セットアップを中止します。	ックする
Advanced Installer <戻るの いってストール(I)	キャンセル

(8) ユーザーアカウント制御が表示された場合は、[はい]をクリックします。



(9) インストールが開始されます。



第8.0版

(10)[完了]をクリックします。



(11)以上で VPN クライアント2のインストールは終了です。 ※再起動は不要です。

5. VPNクライアント2の初期設定

注意:インターネットへ接続した状態で作業を行ってください。

- (1) USB トークンを端末の USB ポートに挿します。
- (2) USB トークンが認識されるとタスクバーのアイコンに「トークンが挿入されました。」と表示されます。(初めて挿入した場合は表示されるまでに時間がかかります)



(3) ルート証明書がインポートされていない場合は"セキュリティ警告"が表示されま すので、[はい]をクリックします。

注意:セキュアネットワークをご利用の Windows アカウントごとに警告が表示されますので、「はい」を選択してください。



(4) [スタート]をクリックし、検索欄に【セキュアネット VPN クライアント2】と入 カし、表示されたアイコンを右クリックし、[ファイルの場所を開く]。



【セキュアネット VPN クライアント2】を右クリックし、「その他のオプション を表示」から[送る] (Windows10 の場合は[送る]のみ) →[デスクトップ(ショート カットを作成)]をクリックする。

(5) デスクトップにショートカットのアイコンが作成されます。



(6) 以上で VPN クライアント2の初期設定は終了です。

※VPN 接続中にファイルサーバやネットワークプリンタをご利用する場合は、以降の 「ローカル LAN アクセスの設定」を実施ください。

● ローカル LAN アクセスの設定

(1) デスクトップのショートカットアイコンをダブルクリックします。



(2) 起動した画面左下のアイコンをクリックします。

🕥 Cisco AnyConnect Secure Mobility Client 📃 🗖 🗙		
	VPN: Connected to Secure_Network_Center. Secure_Network_Center	
00:01:51	IPv4	
\$	a figure	

VPN 接続中にファイルサーバやネットワークプリンタをご利用する場合は "Allowlocal(LAN) access when using VPN(if configured)"にチェックを付けま す。これらにアクセスしない場合はチェックを付ける必要はありません。

注意:設定を有効にしても VPN 接続中はインターネットやネットワーク機器をまたがる(ネットワークアドレスが異なる)ネットワークにはアクセスできません。



(4) "Allowlocal(LAN) access when using VPN(if configured)"にチェックを付け、右上の[×]をクリックします。

🔇 Cisco AnyConnect Secure Mobility Client	-	×
AnyConnect Secure Mobility Client		i
Virtual Private Network (VPN)		
Preferences Statistics Route Details Firewall Message History		
Holminize AnyConnect on VPN connect Alw local (LAN) access when using VPN (if configured) Disable Captive Portal Detection Block connections to untrusted servers		

6. プロキシサーバーの設定

(1) 【Windows11の場合】

「スタート」を右クリックし、「設定」→「ネットワークとインターネット」→「プ ロキシ」→ (プロキシサーバーを使う)「セットアップ」に進む。

	>	
ネットワークとインターネッ	ット › プロキシ	
イーサネットまたは Wi-Fi 接続にプロキシ サーバー 接続にけ適用されません	を使います。これらの設定は、VPN	
自動プロキシ セットアップ		
設定を目動的に検出する	77 CO	
セットアップ スクリプトを使う	tent Tot	
77	291797	
手動フロキシ セットアップ		
プロキシ サーバーを使う オフ	セットアップ	
▲ ヘルプを表示		
■ フィードバックの送信		
	ネットワークとインターネッ イ-サネットまたは Wi-Fi 接続にプロキシ サーバー 接続には適用されません。 自動プロキシ セットアップ 酸定を自動的に検出する セットアップスクリプトを使う オフ プロキシ セットアップ プロキシ セットアップ パー ペールズを表示 デー フィードバックの送信	

【Windows10の場合】

「スタート」を右クリックし、「設定」→「ネットワークとインターネット」→「プロキシ」→画面下部へスクロールする。

設定の検索	イーサネットまたは Wi-Fi 接続にプロキシ サーバーを使います。これらの設定は、VPN 接続にける 田 シカキサム
ヽットワークとインターネット	ブロキシ サーバーを使う
● 状態	オン アドレス ポート
コ イーサネット	8080
🔐 ダイヤルアップ	次のエントリで始まるアドレス以外にプロキシ サーバーを使います。エントリを区切るに はセミコロン (:) を使います。
8° VPN	*.info;*.rece
▶ 機内モード	
リ ^ル モバイル ホットスポット	
⊕ プロキシ	保存
	(金) ヘルプを表示
	フィードバックの送信

(2) 【各 0S 共通】

プロキシサーバーの"プロキシサーバーを使う"のチェックボックスにチェック が付いている場合は(3)に進んでください。チェックが付いていない場合は[キャ ンセル]をクリックして終了してください。設定の必要はありません。

プロキシサーバーを編集	
プロキシ サーバーを使う	
() オン	
ブロキシ IP アドレス ボート	
次のエントリで始まるアドレス以外にプロキシ ロン (;) を使います。	サーバーを使います。エントリを区切るにはセミコ
.info;.rece	
✓ ローカル (イントラネット) のアドレスにはこ	プロキシ サーバーを使わない
保存	キャンセル
【Windows11の画面】	
← 設定	
命 赤-ム	プロキシ
設定の検索	イーサネットまたは Wi-Fi 接続にプロキシ サーバーを使います。これらの設定は、VPN 接続には適用されません。
ネットワークとインターネット	プロキシサーバーを使う
伊 状態	アドレスポート
記 イーサネット	8080
🗊 ศารมหาว	次のエントリで始まるアドレス以外にプロキシ サーバーを使います。 エントリを区切るに はセミコロン (:) を使います。
% VPN	*.info;*.rece
⊸ 機内モード	
(り) モバイル ホットスポット	✓ ローカル (イノトフネット) のアトレスにはノロキン リーバーを使わない
⑦ プロキシ	保存
W 122	
	 ヘルブを表示 フィードバックの注信

【Windows10の画面】

(3) 「次のエントリで始まるアドレス以外にプロキシサーバーを使います。エントリ を区切るにはセミコロン(;)を使います。」の下部の記載欄に以下の通り、記入する。

例外の"次で始まるアドレスにはプロキシを使用しない"に業務システムで使用す るサーバ名または IP アドレスを入力し[OK]をクリックします。複数の接続先を入 力する場合はセミコロン (;)で分けてください。

接続先	設定内容
セキュアネットワークWEBサー	*.info
バ	
オンライン請求システム	*.rece
特定健診保健指導決済システム	
業務システムで使用するサーバ	(接続先ベンダーにお問い合わせください)

プロキシサーバーを編集

プロキシ サーバーを使う

(1) オン	
プロキシ IP アドレス	ポート
なのエントリズかもキマスピースいん	
次のエントリで始まるアトレス以外 ロン (;) を使います。	にノロキシリーバーを使います。エノトリを区切るにはセミコ
.info;.rece	
✓ ローカル (イントラネット) のア	ドレスにはプロキシ サーバーを使わない
保存	キャンセル

~Windows11の画面~

← 設定	
命 赤-ム	プロキシ
設定の検索・	イーサネットまたは Wi-Fi 接続にプロキシ サーバーを使います。これらの設定は、VPN 接続には適用されません。
ネットワークとインターネット	プロキシサーバーを使う
● 状態	アドレス ポート
聖 イーサネット	8080
ล จำานหาว	次のエントリで始まるアドレス以外にブロキシ サーバーを使います。エントリを区切るに はセミコロン () を使います ーー
∞ VPN	*.info;*.rece
☆ 機内モード	✓ ローカル (イントラネット) のアドレスにはブロキシ サーバーを使わない
(中) モバイル ホットスポット	12.77
⊕ プロキシ	17 AU
	♀ ヘルプを表示
	フィードバックの送信

- ~Windows10の画面~
- (4) 以上でプロキシの設定は終了です。

7. VPNの接続方法と切断方法

注意:セキュアネットワークサービスをご利用される Windows アカウント名が日本語 の場合、正常に動作しません。新しく英数字で Windows アカウント名を作成して 下さい。

(例) セキュアネットワークサービス・・・NG SecurenetworkService・・・OK

1. セキュアネットワークへの接続

- ① インターネットへ接続します。
- ② USB トークンを USB ポートに挿します。USB トークンが認識されるとタスクバーのアイコンに「トークンが挿入されました。」と表示されます。



③ デスクトップのショートカットアイコンをダブルクリックします。



 ④ 入力欄に "Secure_Network_Center" が設定されていることを確認し、[Connect] をクリックします。

S Cisco AnyConnect Secure Mobility Client 🗖 🗉 🔀
VPN: Ready to connect. Secure_Network_Center Connect
¢ () *******

⑤ VPN 接続が開始され証明書の確認画面が表示されますので、ユーザ ID を選択し、 [OK]をクリックします。

注意:ユーザ ID (SNU~) 以外の証明書が表示される場合があります。ユーザ ID

(SNU~)を正しく選択してください。
Windows セキュリティ
証明書の確認 [OK] をクリックして、この証明書を確認します。この証明書が正しくな い場合、[キャンセル] をクリックしてください。
SNUTION NUTION
ОК ТУХЕЛ

 ⑥ VPN 接続が開始され認証画面が表示されるので、ユーザ PIN (パスワード)を入 力し、[ログイン]をクリックします。

ユーザPIN	x
Q ユーザPINを認証します:	
ユーザPIN:	
🔲 ソフト キーボード	
ユーザPINの変更 ログイン キャンセル	

 ⑦ 正しいユーザ PIN (パスワード) を入力すると VPN 接続が確立します。その後 VPN クライアント2の画面が自動的に閉じ、タスクバーに青いアイコンが表示されます。



2. セキュアネットワークの接続の確認

 ブラウザを起動し、セキュアネットワークインフォメーションサイト (http://www.info)に接続します。

ブページ ロサービス機要 ロドキュメント ロ: www.info	/フトウェ:	ダウンロード BQ&A B接触情報一覧	[お気に入り]に追加して
お知らせ		稼働情報	おく事をお勧めします。
0016年2月28日 【基幹設備メソラナソスのお知らせ】 1メソラナンス目時 3.373年3)210~1月 400	^	・特定検診・特定保健指導共同情報処理システム、 しセフトオンライン意味システム及びその他の医療 機関向サシステムの稼動情報は各ペンダーまでご確認をお願いします。	
2.5~ビス.停止時間 3/23(金) 22:00~翌 2:00(予定)		・セキュアネットワークサービスは正常に稼働してい ます。	
3内容 上記の時間帯でセキュアネットワークサービス基幹設置のパンラ を実施します。サービス停止時間帯はサービスのご利用ができま	ナンス せん。	R動情報一覧	
2017年9月8日 【メンテナンスのお知らせ】			
1.メンテナンス日時 8/21(木) 18:00~22:00			
2.インフォメーションサイト停止時間 18:00~21:30(予定)			

② オンライン請求システム、特定健診保健指導決済システムまたは業務システムに 接続して下さい。

接続方法やご利用方法は各システムのマニュアルをご参照下さい。

第8.0版

3. セキュアネットワークからの切断

① デスクトップのアイコンをダブルクリックします。



② [Disconnect] \mathcal{E} \mathcal{D} \mathcal{D}



③ 切断後はタスクバーに赤いアイコンが表示されます。



④ VPN クライアント2を終了する場合は、タスクバーの赤いアイコンを右クリックし、[Quit]をクリックします。



8. 接続できない場合

接続できない例を挙げています。その他の本ソフトの詳細な使用方法・接続不具合への対 処については、本ソフトのヘルプ機能をご参照願います。

(1) "Certificate Validation Failure" (図 8-1) が表示され、接続できない。



- USBトークンを挿し直してルート証明書をインポートして下さい。
 (参考:5-(3), VPNクライアント2の初期設定)
- (2) "ユーザ PIN が正しくありません。~"(図 8-2) が表示され、接続できない。



ユーザPIN(パスワード)が誤っています。正しいユーザPINを入力して 下さい。

注意:ユーザPINを忘れた場合は、弊社まで USB トークンを返送して頂く必要があります。弊社コールセンターでは ID やユーザPINはセキュリティ上ー 切お答えできません。 (3) "Could not connect to server.~"(図 8-3) が表示され、接続できない。



▶ インターネットに正常に接続できている事を確認して下さい。

<確認方法例>

ブラウザを起動させて、インターネット上のホームページが表示可能かどうか を調べて下さい。(例) http://www.yahoo.co.jp

<結果&対処方法>

結果1:ホームページが表示できない。

インターネットの接続がうまくいっておりません。インターネットの 接続環境を確認して下さい。

結果2:ホームページが表示できた。

接続エントリのプロパティの名称が正しいか確認して下さい。

(参考: 5. VPNクライアント2の初期設定)

S Cisco AnyConnect Secure Mobility Client	
VPN: Ready to connect Secure_Network_Center	Connect
\$ (i)	n <mark>e</mark> gor

• **IP**アドレスが正しい場合

ADSL ルータやクライアントに設定しているファイアウォールソフトなど によって、通信で利用する UDP ポートが制限されている可能性があります。 必要なポートが制限されていないか確認をお願い致します。特に、UDP 500 と UDP 4500 および TCP 443 の通信ポートが正常に通過できる設定が必要で す。(参考: 11-(2))

機器の設定や端末の設定については、機器の購入先のベンダーまたはメー カーまでお問合せをお願い致します。

- ウイルス対策ソフトまたは Windows ファイアウォールの設定を変更して下さい。(Windows ファイアウォールの設定は次項をご参照下さい)。
 - * 以下は主なウイルス対策ソフトの設定をご紹介しています。その他の製品も 同様の対応が必要となる場合があります。(弊社では個別の製品の対応は致 しておりません)
 - ウイルスバスタークラウドの設定
 - ウイルスバスタークラウドを起動します。
 - ② [設定]アイコンをクリックします。



③ [例外設定]をクリックします。



④ [追加]をクリックします。



⑤ [参照]をクリックします。

コンピュー	タの保護設定 ····································
▶ ウイルス/ス	ノイウェア対策 フェキャン、やを担かれた除死するファイルノフォルズを設定します。 項目の追加
▼ 例外設定	ファイルやフォルダを追加するには、【参照…】をクリックします。
2741	
Webサイ	
無線LAN	
70/hb	ок ++>th
	明設定に戻す OK キャンセル 適用

⑥ "C:¥Program Files¥Cisco"を選択し、[開く]をクリックします。



⑦ [OK]をクリックします。

コンピュー	タの保護設定人	' _ ×
▶ ウイルスバス	パイウェア対策 フキャンや影響の対象が高時外はスファイル/フォルガを設定します。	,
▶ 有害サイト		
▼ 例外設定	ジティルシスルシスニュージョンには、「mmm」でフララフラムタ。	
0 ファイル		
Web U -		
無線LAN		
その他の	ОК <u></u> <i>†<i>т</i>><i>ти</i></i>	
すべて初期	朝設定に戻す OK キャンセル 適	
C		

⑧ [OK]をクリックします。

コンピュータの保護設定		? <u>-</u> ×
▶ ウイルス/スパイウェア対策	スキャンや監視の対象から除外するファイルノフォルタ	ダを設定します。
▶ 有害サイト/迷惑メール対策		
▼ 例外設定	C:XProgram EilaeXCisco	<u>917</u> ⊐+∥4
@ ファイルフォルダ		51105
Webサイト		
無線LANアドバイザ		
その他の設定		
すべて初期設定に戻す	OK キャンセル	適用

⑨ 以上で終了です。

- Windows ファイアウォールまたはファイアウォールソフトの設定を変更して 下さい。(ウイスル対策ソフトの設定は前項をご参照下さい)
 - Windows 11/10/8.1/8の Window ファイアウォールの設定
 - 「設定」→「コントロール パネル」→「Windows ファイアウォール」を開き、「Windows ファイアウォールを介したアプリまたは機能を許可」をクリックします。

@	Windows ファイアウォール	_ _ ×
€ 🦻 🔹 ↑ 🔮 « ₫ぺႠの⊐>H	ロール パネル項目 → Windows ファイアウォール	✓ ○ コントロール パネルの検索
コントロール パネル ホーム	Windows ファイアウォールによる PC の保護	ξ.
Windows ファイアウォールを介した アプリまたは機能を許可	Vindows ファイアウォールによって、ハッカーまたは悪意のあ t スを防止できるようになります。	5るソフトウェアによるインターネットまたはネットワークを経由したアク
6 BARREWER	プライベート ネットワーク(<u>R</u>)	接続されていません 🕑
 Windows ファイアウォールの有効 化または無効化 	✓ ゲストまたはパブリック ネットワーク(E	2) 接続済み 🕥
 9 既定値に戻す ※ 詳細設定 	空港、喫茶店など、公共の場のネットワーク	
ネットワークのトラブルシューティング	Windows ファイアウォールの状態:	有効
	著信接続:	許可されたアプリの一覧にないアプリへのすべての接続をブロッ クする
	アクティブなパブリック ネットワーク:	〒 ネットワーク
	通知の状態:	Windows ファイアウォールが新しいアプリをブロックしたときに 通知を受け取る
腿連項目		
アクション センター		
ネットワークと共有センター		

② 「設定の変更」→「別のプログラムの許可」をクリックします。



- セキュアネットワークサービスご利用マニュアル (USB トークン)
 - ③ 「VPN クライアント2」を選択し、[追加]をクリックします。

④ もう一度、[OK]をクリックして終了です。

▶ デフォルトゲートウェイが設定されているか確認してください。

<確認方法例>

Windows 付属のコマンドプロンプトを起動し、"ipconfig /all"と入力して下さ い。Default Gateway が空白の場合や IP Address が"169.254.x.x"(x は 0~ 255 の数字)の場合は DHCP サーバ、ブロードバンドルータや PC の TCP/IP の設定をご確認下さい。

イーサネット アダプター ローカル エリア接続:
<u>接続固有の DNS サフィックス .</u> : IPv4 アドレス
<u>サブネット マスク</u> デフォルト ゲートウェイ
イーサネット アダプター WAN:
接続固有の DNS サフィックス : IPv4 アドレス : サブネット マスク : デフォルト ゲートウェイ :
イーサネット アダプター Bluetooth ネットワーク接続:

(4) "Reconnect, waiting for network connectivity..." (図 8-4) が表示される。

Cisco AnyC	Connect Secure Mobility Client	
	VPN: Contacting Secure_Network_Center.	図 8-4
\$ (i)		
 インター て下さい 	ーネットが切断されました。インターネット い。	▶接続状態を確認し再接続

(5) "The IPsec VPN connection was terminated due to an authentication failure or timeout.~"(図 8-5) が表示され、接続できない。



- USBトークンが取り外されたまま、接続をした場合に表示されます。 正しく取り付けて再接続をしてください。
- (6) "Your VPN connection has exceeded the session time limit.~"(図 8-6) が表示 され、切断された。



規定の連続接続時間を過ぎた場合に表示されます。必要に応じて再接続をして 下さい。 (7) "Your VPN connection has been terminated due to inactivity.~"(図 8-7) が表示され、切断された。



て下さい。

(8) "VPN connection terminated, smart card removed from reader." (図 8-8) が表示され、切断された。



- USBトークンが抜けています。VPN クライアントを終了し、USBトークンの 挿入先ポートを変更して再接続して下さい。
- > USB ハブを使わずに直接 PC に挿入して下さい。

 (9) "Establishing VPN session…"(図 8-9) が表示中のまま VPN 接続処理が進まず、 エラーメッセージも表示されない。

S Cisco AnyCo	onnect Secure Mobility Client 📃 🗖 🗙	
	VPN: Contacting Secure_Network_Center.	図 8-9
	Secure_Network_Center Connect	
Q ()		

- VPN プロファイルが変更されている可能性があります。VPN プロファイルの 内容を確認し、再接続して下さい。
- 本画面を終了する場合には、タスクバーの赤いアイコンを右クリックし、[Quit] をクリックしてください。

(10) 正常にログインできるが、サーバに接続できない。

ご利用するサーバに対して通信確認を行なって下さい。
<確認方法例>

Windows 付属のコマンドプロンプトを起動し、"ping *IP アドレス*"と入力して下さい。(IP アドレス部分は接続したいサーバの IP アドレス)

(入力例:セキュアネットワークインフォメーションサイト)>ping

```
202.228.11.110
```

📷 管理者: コマンド プロンプト	X
Microsoft Windows [Version 6.1.7601] Conversion: All sights recorded and the second se	Â
copyright (c) 2000 wherosoft corporation. All rights reserved.	
C:¥Users¥snet>ping 202.228.11.110	
202.228.11.110 に ping を送信しています 32 バイトのデータ:	
202.228.11.110 からの応答: バイト数 =32 時間 =25ms TTL=64 202.228.11.110 からの応答: バイト数 =32 時間 =25ms TTL=64	
202.228.TL.TTU からの応合: ハイト数 =32 時間 =20ms TTL=64 202 228 11 110 からの広答: バイト数 =32 時間 =16ms TTL=64	
202.228.11.110 からの応答: バイト数 =32 時間 =14ms TTL=64	
202.228.11.110 の ping 統計:	
- バケット数:送信 = 4、受信 = 4、損失 = 0(0%の損失)、 ニウンビートリップの押貨時間(ミリか):	
レリンド ドリッフの概算時间(ミリ科ル 最小 = 14ms、最大 = 25ms、平均 = 18ms	
C:¥Users¥snet>	

<結果&対処方法>

- 結果1: "Reply from IP アドレス: bytes=32 time=×ms"と表示される。
 ① 正常に通信できております。端末のアプリケーションの設定を確認して下さい。
- ③ MTU 値(通信時のパケットサイズ)が適切でない場合があります。設定 を確認してください。
- 結果2: "Request time out"と表示される。

対象のサーバがダウンしているか、もしくは通信経路に異常が見られ ます。

注意:対象のサーバがセキュリティ上 ping 応答を返さない設定となっている 場合もあります。その場合も結果2と同一の現象が発生します。対象のサーバが ping 応答を返す設定となっているかどうかはサーバの管理者に問い合わせを お願い致します。

- (11) Administrator 権限の ID/パスワード入力を求められ(図なし)、インストールで きない。
 - User 権限や Power User 権限ではインストールできません。Administrator 権 限でインストールして下さい。
- ◆ その他 (ルータの問題)
 - IPSec パススルー / VPN パススルー 接続できない場合でご使用のルータに IPSec パススルー機能や VPN パスス ルー機能がある場合は有効にして下さい。
 - ファームウェアのバージョンアップ ルータをご利用の場合においてルータのファームウェアをバージョンアップ した事で不具合が解消される場合があります。アップデート方法や詳細につい ては購入元やメーカーまでお問合せ下さい。
 - ▶ ブリッジモード

ADSL ルータにブリッジモードの機能がある場合は設定しますと利用可能に なる場合があります。ただし、ルータ1台につき端末1台の利用となります。 設定方法は ADSL ルータのマニュアルをご確認下さい。

9. VPNクライアント2のアンインストール

 [スタート]→[コントロールパネル]→[プログラムのアンインストール]の順にク リックして起動します。



(2) "Cisco AnyConnect Secure Mobility Client"を選択し、[アンインストール]をク リックします。



(3) 確認画面が表示された場合は[はい]をクリックします。



(4) アンインストールが開始されます。



(5) "ユーザーアカウント制御"が表示された場合は[許可]をクリックします。

	ユーザー アカウント制御	
	認識できないプログラムがこのコンピュータへのアクセスを要求しています	
	発行元がわかっている場合や以前使用したことがある場合を除き、このプログ ラムは実行しないでください。	
	■ 認識できない発行元	
	◆ キャンセル このプログラムの発行元も目的ちわかりません。	
(◆許可(A) このプログラムを信用します。発行元がわかっているか、このプログラ ムを以前使用したことがあります。	\triangleright
	♥ 詳細(D)	
	ユーザー アカウント制御は、あなたの許可なくコンピュータに変更が適用される のを防ぎます。	

(6) アンインストールが継続されます。



(7) コントロールパネルのプログラムと機能の画面から"Cisco AnyConnect Secure Mobility Client"が消えていればアンインストールは終了です。



(8) デスクトップのアイコンを手動で削除して下さい。



(9) 以上で VPN クライアント2のアンインストールは終了です。

10. USBトークンドライバのアンインストール

(1) アンインストーラを起動します。

USB トークン (緑): [スタート]→[コントロールパネル]→[ePass2003]を右クリ ックし、[アンインストール] の順にクリックして起動しま す。

$\rightarrow \cdot \wedge \square \cdot \square \cdot$	パロール パネル > すべてのコントロール パネル項目 > プログラムと機能				~ C	プロ
コントロール パネル ホーム	プログラムのアンインストールまたは変更					
インストールされた更新プログラムを 表示	プログラムをアンインストールするには、一覧からプログラムを選択して [ア	ンインストール]、[変更]、または [修復] をクリッ	クします。			
Windows の機能の有効化または						
無効化	整理 ▼ アンインストール					
	名前	発行元	インストール日	サイズ	パージョン	
	ePass2003	EnterSafe	2022/10/21		1.1.14.813	
	HP Connection Opt アンインストール(U)	HP	2022/03/30		2.0.19.0	
	1 HP Documentation	HP Inc.	2022/05/10		1.0.0.1	
	MP Notifications	HP	2022/03/30	18.7 MB	1.1.28.1	
	HP Security Update Service	HP Inc.	2022/05/10		4.3.7.346	
	SHP Wolf Security	HP Inc.	2022/03/30	614 MB	4.3.4.610	
	res los	HP Inc.	2022/03/30	183 MB	1.00.0000	
	C Microsoft Edge	Microsoft Corporation	2022/03/30		92.0.902.67	
	Microsoft OneDrive	Microsoft Corporation	2022/06/10	242 MB	22.099.0508.0001	
	Microsoft Update Health Tools	Microsoft Corporation	2022/06/10	0.99 MB	4.67.0.0	
	Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32	Microsoft Corporation	2022/10/06	20.1 MB	14.32.31332.0	
	(Npcap	Nmap Project	2022/10/06		1.71	
	Kealtek USB Audio	Realtek Semiconductor Corp.	2022/03/30		6.3.9600.250	
	Tera Term 4.106	TeraTerm Project	2022/09/25	13.3 MB	4.106	
	Windows 11 インストール アシスタント	Microsoft Corporation	2022/05/10	5.00 MB	1.4.19041.1610	
	❤ Windows PC 正常性チェック	Microsoft Corporation	2022/05/10	11.6 MB	3.7.2204.15001	
	Wireshark 4.0.0 64-bit	The Wireshark developer community,	2022/10/06	201 MB	4.0.0	

(2) ユーザーアカウント制御が表示された場合は、[はい]をクリックします。



(3) [アンインストール]をクリックします。



(4) アンインストールが開始されます。



(5) アンインストール終了後、[完了]をクリックします。



(6) 再起動後、USB トークンドライバのアンインストールは終了です。

11. 注意事項

(1) VPN 通信中の動作について

- ① 厚生労働省のガイドラインによりセキュアネットワークサービスではクライアン ト/サーバ間は HTTP、HTTPS 及び ICMP のみ通信を許可しています。クライアント同士の通信は許可していません。その他の通信ポートをご利用になられる場合 やクライアント同士の通信が必要な場合は予めご連絡して頂き個別に対応させて 頂きます。
- ② セキュアネットワークサービスのご利用中(VPN クライアントソフトの起動中)は、 通常のインターネット(Web閲覧等)及び社内ネットワーク(ファイルサーバや ネットワークプリンタ等)には接続できません。ファイルサーバやネットワーク プリンタをご利用になる場合は"ローカル LAN アクセスの設定"を行ってください。(参考:5)尚、インターネットをご利用になる場合はセキュアネットワーク サービスを切断(VPN クライアントソフトを終了)して下さい。
- ③ セキュアネットワークサービスのご利用中は、"無通信接続時間 30 分 "または "連続接続時間 8 時間"を過ぎますと、強制的に VPN セッションが切断されますのでご了承下さい。

(2) VPN クライアントの通信フローについて

VPN クライアントソフトは、端末が NAPT 環境下であっても非 NAPT 環境であっ ても、同じ接続方法(UDP:500、4500 使用)にて接続されます。VPN クライアントソ フトの [Statistics] タブの"Transport Information"の"Protocol"の項目に "IKEv2/IPSec NAT-T"と表示されます。

統計情報の表示

VPN 接続中に GUI 右下のアイコンをクリックし、[Statistics]タブをクリック します。クライアントに割り当てられた IP アドレスや接続時間等が表示されま す。



S Cisco AnyConnect Secure Mobility Client								
*********** AnyConnect Secure Mobility Client								
Virtual Private Network	(VPN)							
Preference. Statistics Pout	e Details Firewall Message History							
		A						
Connection Information	 	_						
State:	Connected	E						
Tunnel Mode (IPv4):	Tunnel All Traffic							
Tunnel Mode (IPv6):	Drop All Traffic							
Dynamic Tunnel Exclusion:	None							
Duration:	00:00:20							
Address Information —	None	_ ^						
Client (IPv4):	172.31.8.167							
Client (IPv6):	Not Available							
Server:	202.228.11.1							
Bytes		_ ^						
Sent:	10965	-						
	Reset Exp	ort Stats						

NAPT 環境及び非 NAPT 環境のどちらの場合でも、同じ方式で接続されます。 NAPT 環境では、UDP パケットを NAPT 透過させるために、VPN クライアントから の通信を通信セッション毎にポート番号を非特権ポート(1024 以上)に変化します。通 信設計を行なう場合、以下を参照して適切なアクセス制御を行って下さい。

個々の機器の設定や端末の設定については、機器の購入先のベンダーやメーカーま でお問合せ頂きますようお願い致します。

(上記の動作は、本ソフトの独自仕様ではなく、通信に UDP を利用して NAPT を透 過させるための一般的な方法です。)

a. VPN 通信のアクセス制御の設定について

UDP 通信の特性により、ルータ及びファイアウォール(F/W)で下記の通信が確 立できる設定が必要となる場合があります。

	番号	通信方向	宛先 ポート	送信元 ポート	アクセス 制御	
	1	セキュアネットワークセンター 🖛 ルータ・F/W(VPNクライアント	UDP 500	UDP 1024以上	許可	
	2	セキュアネットワークセンター 🖛 ルータ・F/W(VPNクライアント	UDP 4500	UDP 1024以上	許可	
	3	セキュアネットワークセンター 🖛 ルータ・F/W(VPNクライアント	TCP 443	TCP 1024以上	許可	
	4	セキュアネットワークセンター ➡ ルータ・F/W(VPNクライアント	UDP 1024以上	UDP 500	許可	
	5	セキュアネットワークセンター ➡ ルータ・F/W(VPNクライアント	UDP 1024以上	UDP 4500	許可	
	6	セキュアネットワークセンター ➡ ルータ・F/W(VPNクライアント	TCP 1024以上	TCP 443	許可	

※基本的に ステートフル パケット インスペクション が実装されているルータ 及びファイアウォールには下記の④~⑥の設定は不要です。

b. 端末通信する場合の通信シーケンス

①主に使用される環境

*

- ・ADSL/FTTH でブロードバンドルータ経由インターネット接続
- ・ケーブル TV インターネット接続
- ・ファイアウォール経由専用線インターネット接続 等

第8.0版

②通信シーケンス

セキュアネットワークセンターが利用する通信ポート

UDP 500 UDP 4500 TCP 443 (プロファイルダウンロードのみに使用) 通信を透過させるために、クライアントからセキュアネットワークセンターへのクラ イアントソースポート番号は 1024~65535 まで任意に変化します。 ルータからグローバル IP アドレスへ送信する際にさらにルータ内部でソースポートは 非特権ポートに変換されます。

<通信例>			
セキュアネット ワークセンター Internet	ルータ・F/W NAPT	VPN クライアント	
202.228.11.1 200.	200.200.1 192.168	3.1.1 192.168.1.2 (7° 7	パヘ゛ートアト゛レス)
	機器により任意に始点のポート番号が非特権ポート変換されが ローパ WTト ひえで送信される。 (変換前と後をテーブルに保存)		
始点 200.200.200.1 11026 終点 202.228.11.1 500	始点 200.200.200.1 11026 (前:192.168.1.2 1026) 終点 202.228.11.1 500	◆ 始点 192.168.1.2 1026 終点 202.228.11.1 500	
始点 202.228.11.1 500 終点 200.200.200.1 11026	▶ 始点 202.228.11.1 500 終点 192.168.1.2 1026 (前 200.200.200.1 11026)		
	戻りのパケットに対し、テーブ ルを参照し、アドレス・ポート 番号を元の番号に書き換える。		UDP 500 での通信
始点 200.200.200.1 11026 終点 202.228.11.1 500	- 始点 200.200.200.1 11026 (前:192.168.1.2 1026) 終点 202.228.11.1 500	始点 192.168.1.2 1026 終点 202.228.11.1 500	
始点 202.228.11.1 500 終点 200.200.200.1 11026	▶ 始点 202.228.11.1 500 終点 192.168.1.2 1026 (前 200.200.200.1 11026)	→ 始点 202.228.11.1 500 終点 192.168.1.2 1026	
始点 200.200.200.1 11027 終点 202.228.11.1 4500	- 始点 200.200.200.1 11027 (前:192.168.1.2 1027) 終点 202.228.11.1 4500	始点 192.168.1.2 1027 終点 202.228.11.1 4500	UDP 4500 での通信
L 始点 202.228.11.1 4500 終点 200.200.200.1 11027	 ▶ 始点 202.228.11.1 4500 終点 192.168.1.2 1027 (前 200.200.200.1 11027) 	始点 202.228.11.1 4500 終点 192.168.1.2 1027	
I			

(4) 海外への持ち出しについて

注意:セキュアネットワークサービスは日本国内からのご利用に限定していますので海外 からご利用できません。以下は VPN クライアントソフトをインストールしたパソコンを 海外に持ち出す場合においての手続き方法であり、海外からのご利用が可能である事を示 すものではありません。

■ 弊社の役割

VPN 等、データの暗号化を行う製品を海外に持ち出す場合、輸出・輸入の手続きが 必要です。エンドユーザが製品を海外に持ち出す際、これらの手続きはエンドユーザ 責任で行っていただくことになっています。

弊社の役割としては、エンドユーザ様が要求された「該非判定書(パラメータシート)」 をメーカーに対し作成依頼します。

該非判定書(パラメータシート)の入手には2週間を要します。あらかじめご留意下 さい。

∎ 参考

<暗号化モジュール輸出に関する問合せ窓口>

・経済産業省 貿易経済協力局 貿易管理部 安全保障貿易審査課
 TEL: 03-3501-2801

http://www.meti.go.jp/policy/anpo/index.html

・財団法人 安全保障貿易情報センター

TEL: 03-3593-1147

http://www.cistec.or.jp

<暗号化モジュールの輸出先国の輸入制限問い合わせ窓口>

 日本貿易振興機構 貿易投資相談センター 貿易投資相談課 TEL:03-3582-5171
 E-mail:bua-ref@jetro.go.jp
 https://www.jetro.go.jp/services/advice/