

セキュアネットワークサービス

VPN クライアント 2 版

ご利用マニュアル

(USB トークン)

<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-1	9
	VPN クライアント 2 のインストール-2	13
5.	VPN 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.....	29
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.....	46

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

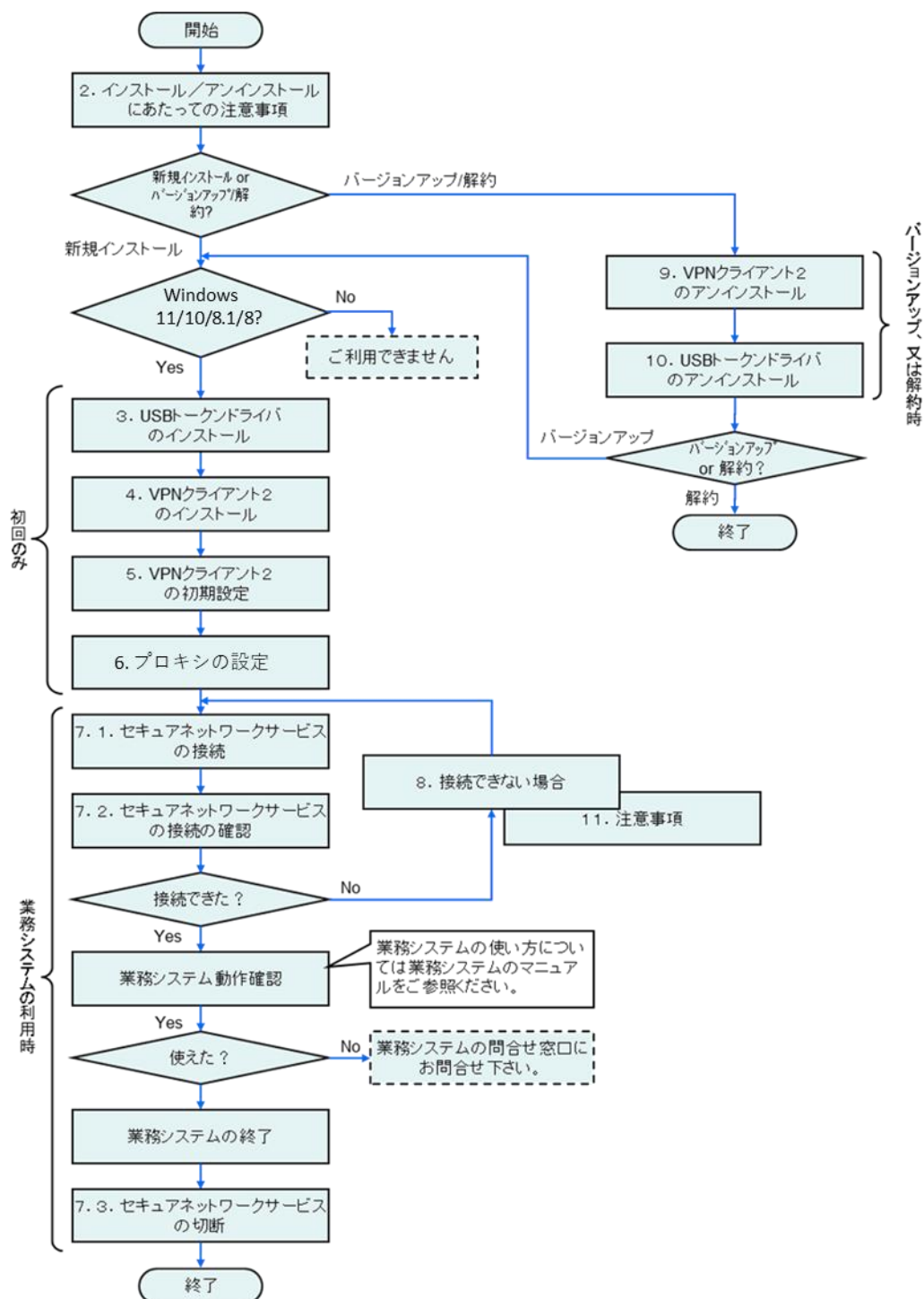
その他：Microsoft インストーラー3.1 が利用可能であること

●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ください。

(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。

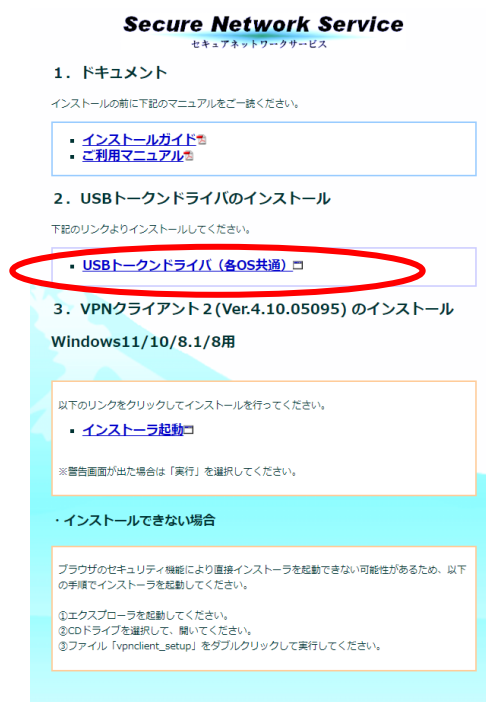
(例) セキュアネットワークサービス・・・NG SecurenetworkService・・・OK

(5) 対応 USB トークン

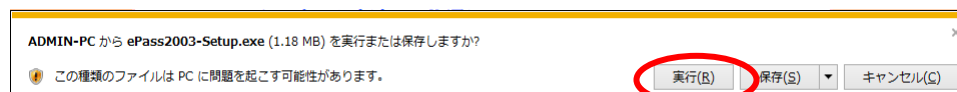
青色 USB トークンは Windows 10/11 ではご利用いただけません。緑色 USB トークンに交換が必要です。詳細は購入元へお問い合わせ下さい。

3. USB トークンドライバのインストール

- (1) 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)



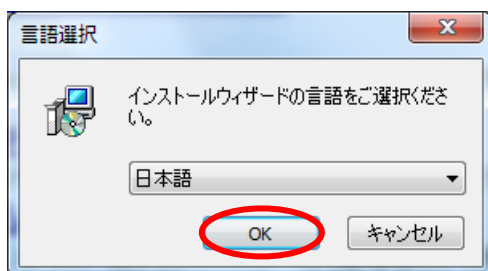
- (4) セキュリティ警告が表示された場合は、[保存]をクリックします。



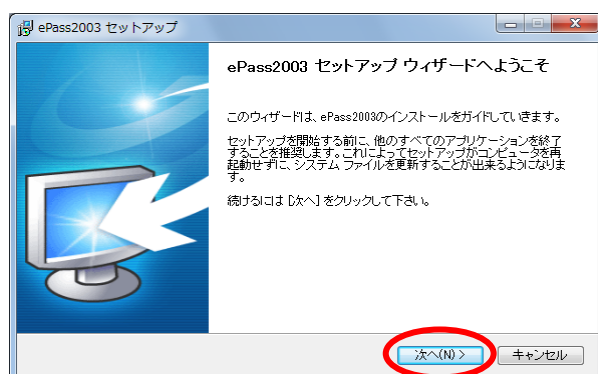
- (5) ユーザーアカウント制御が表示された場合は、[はい]をクリックします。



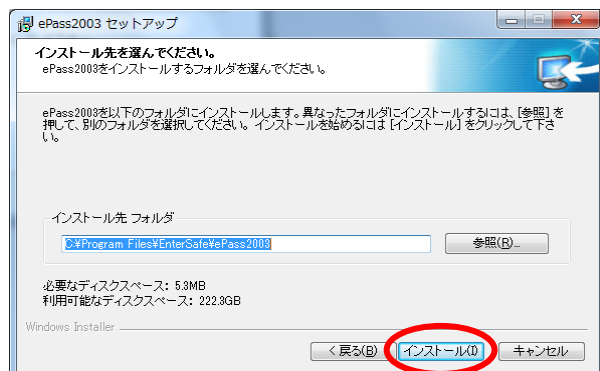
- (6) “日本語” を選択し、[OK]をクリックします。



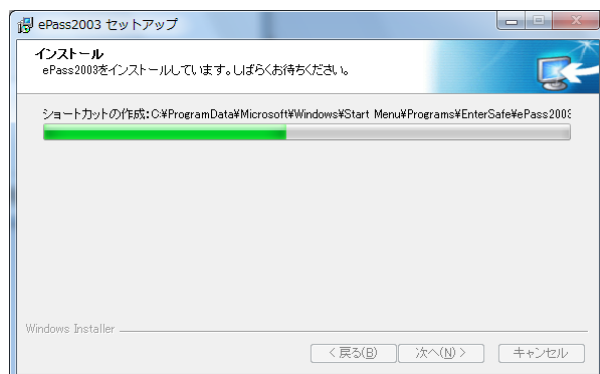
- (7) インストーラが実行されますので[次へ]をクリックします。



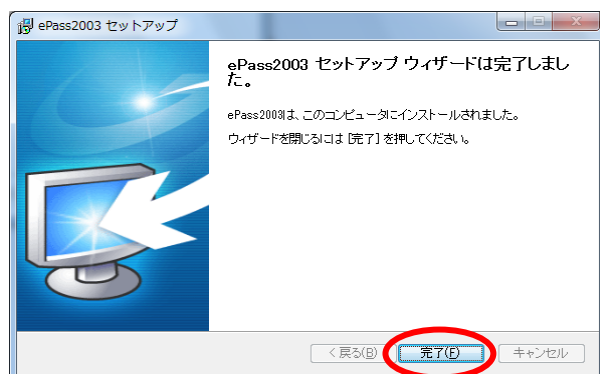
(8) [インストール]をクリックします。



(9) インストールが開始されます。



(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。

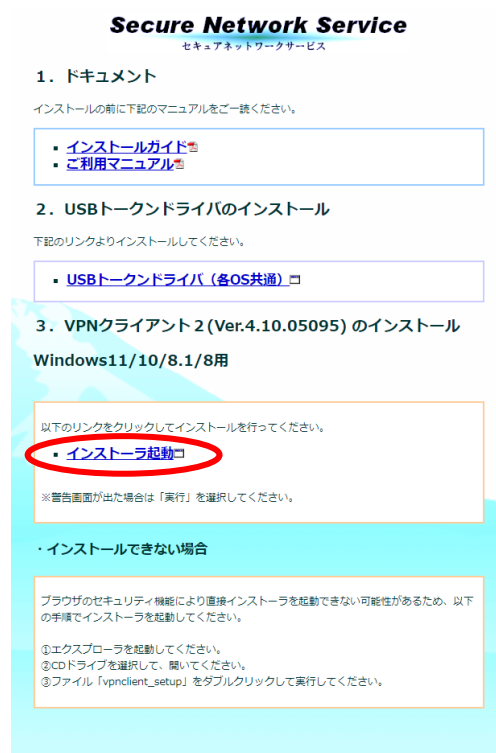
注意：Windows 9x/ME/2000/XP/Vista/ServerOS には対応していません。

Windows 7/7 Starter Edition、Windows RT には対応していません。

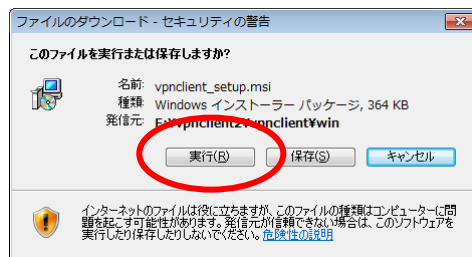
アップグレードした OS には対応していません。

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。

- (1) 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 “[インストーラ起動](#)” をクリックします。



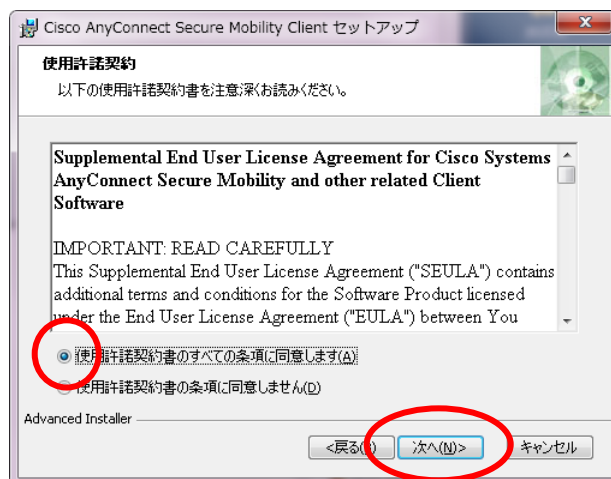
- (3) セキュリティの警告が表示された場合は、[実行]をクリックします。



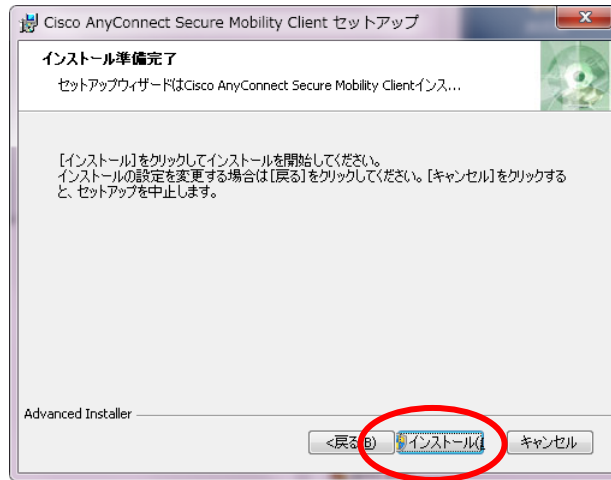
- (4) インストーラが実行されますので[次へ]をクリックします。



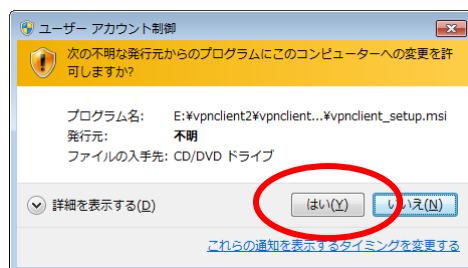
- (5) “使用許諾契約書のすべての条項に同意します(A)”を選択し、[次へ]をクリックします。



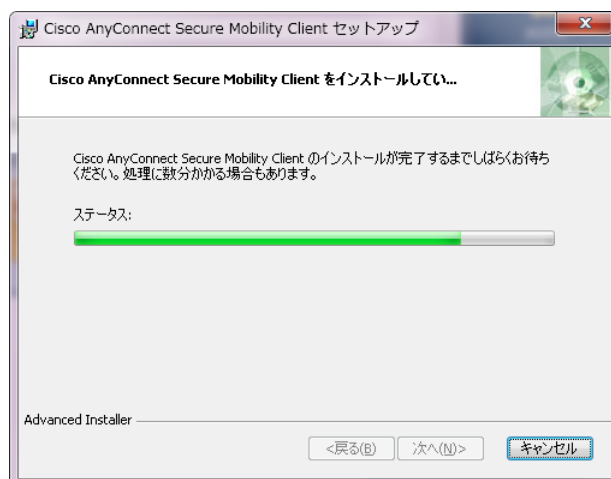
- (6) [インストール]をクリックします。



- (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。



- (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。



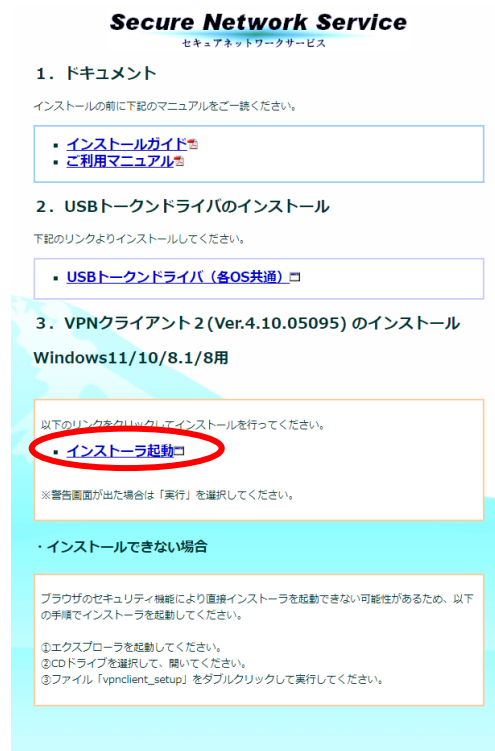
- (10) 以上で VPN クライアント 2 のインストールは終了です。

※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

- (1) 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。)



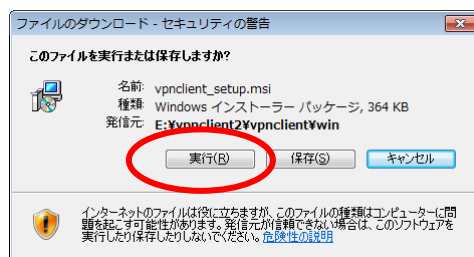
- (2) Windows エクスプローラから CD-ROM の入った CD/DVD ドライブをクリックします。



- (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.txt	2022/10/28 9:15	テキストドキュメント	1 KB
vpnclient_setup.msi - ショートカット (circled in red)	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。



- (5) 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。



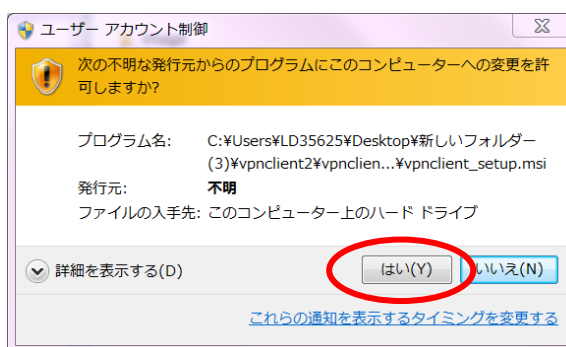
- (6) “使用許諾契約書のすべての条項に同意します(A)”を選択し、[次へ]をクリックします。



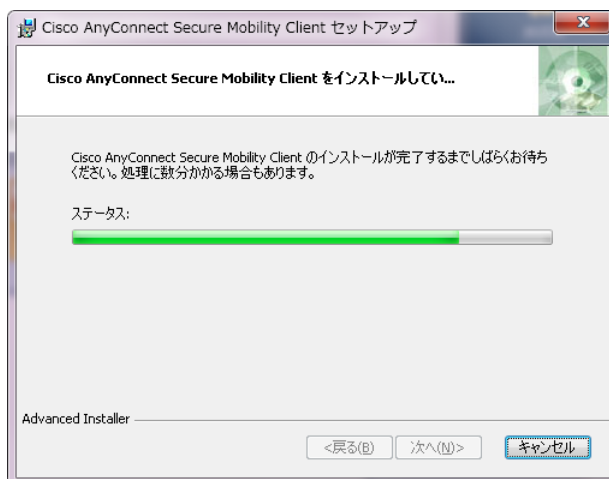
- (7) [インストール]をクリックします。



- (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。



(10)[完了]をクリックします。



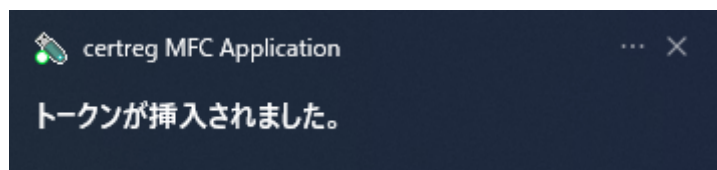
(11)以上でVPNクライアント2のインストールは終了です。

※再起動は不要です。

5. VPNクライアント2の初期設定

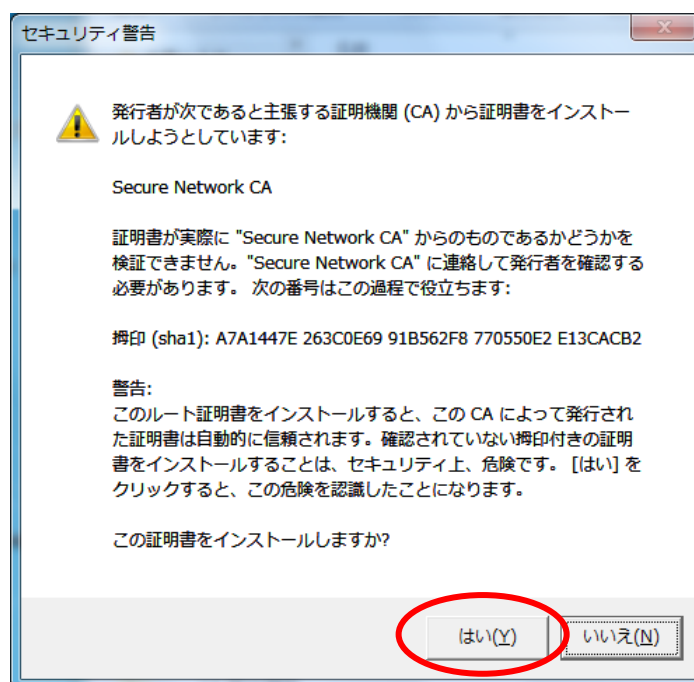
注意：インターネットへ接続した状態で作業を行ってください。

- (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)

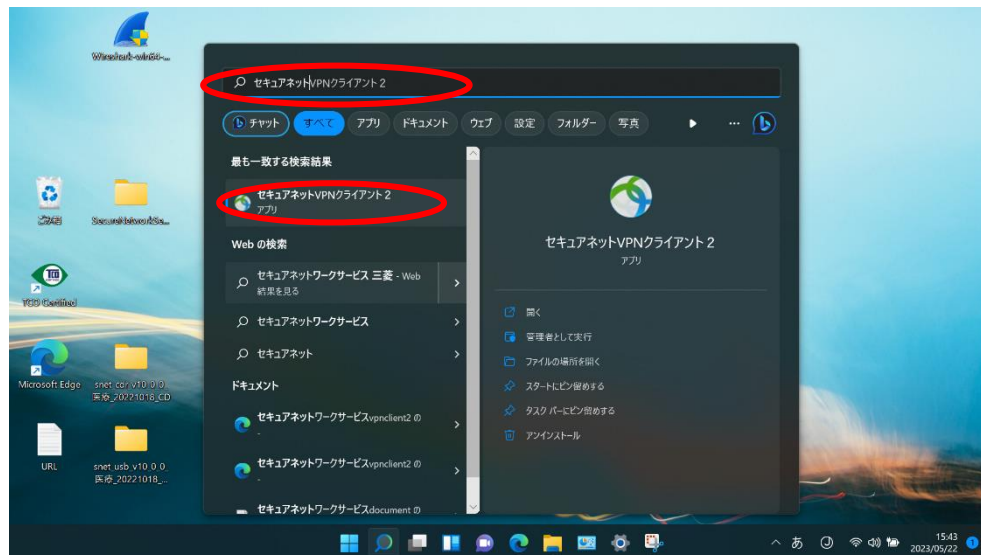


- (3) ルート証明書がインポートされていない場合は“セキュリティ警告”が表示されますので、[はい]をクリックします。

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】と入力し、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。

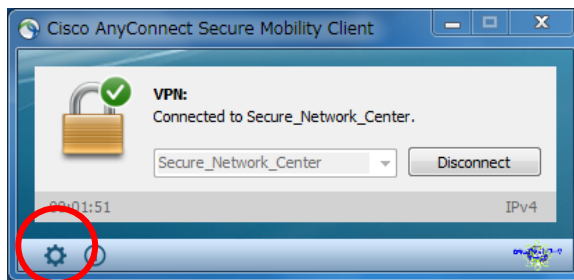
※VPN 接続中にファイルサーバやネットワークプリンタをご利用の場合は、以降の「ローカル LAN アクセスの設定」を実施ください。

● 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。



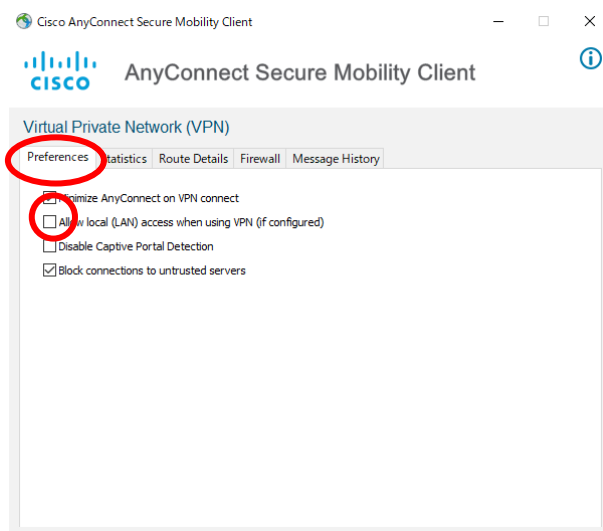
- (2) 起動した画面左下のアイコンをクリックします。



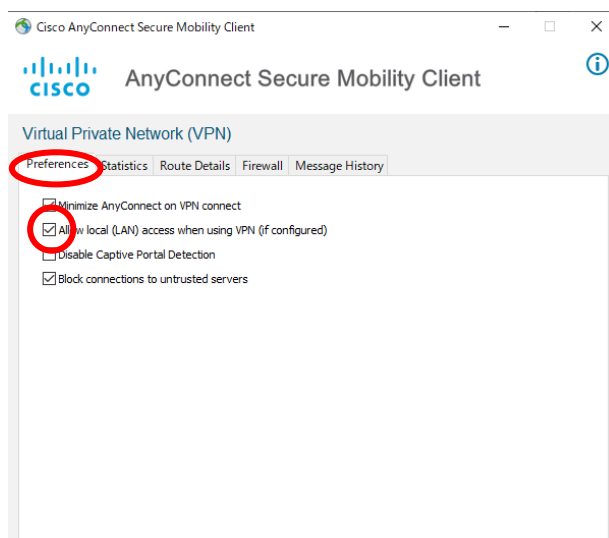
- (3) “Preferences” タブをクリックします。

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
“Allow local (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) “Allow local (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。



6. プロキシサーバーの設定

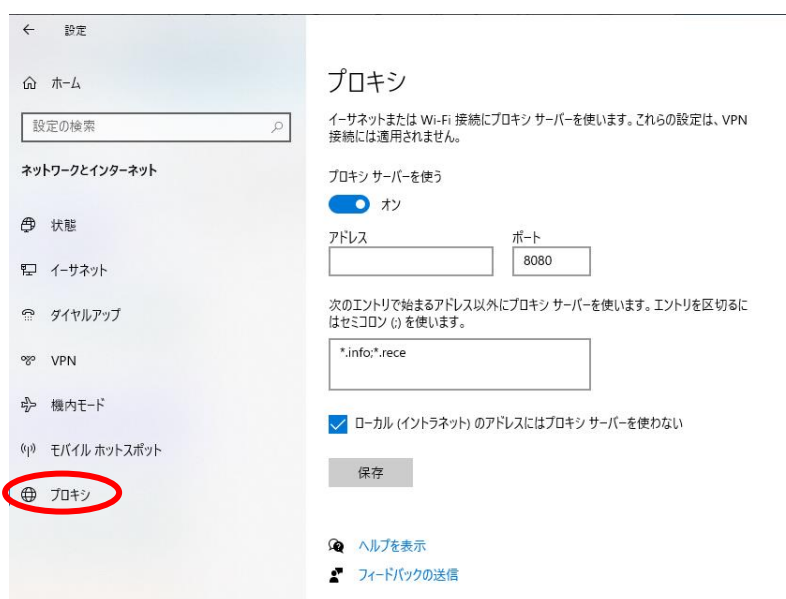
(1) 【Windows11 の場合】

「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。



【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。



(2) 【各 OS 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

プロキシ IP アドレス

ポート

8080

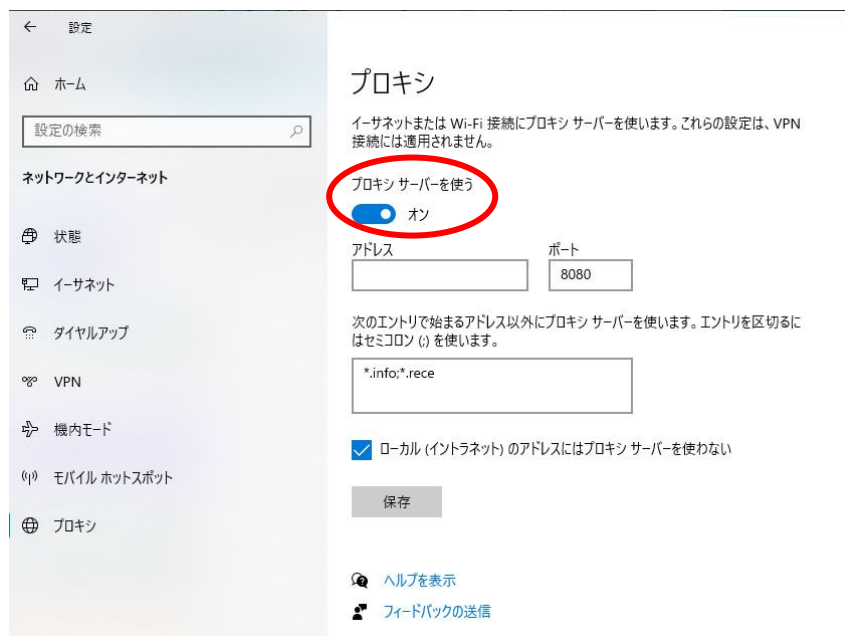
次のエントリで始まるアドレス以外にプロキシ サーバーを使います。エントリを区切るにはセミコロン (;) を使います。

☒ 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】



【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サーバ	*.info
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	*.rece
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

☒ オン

プロキシ IP アドレス

ポート

8080

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。

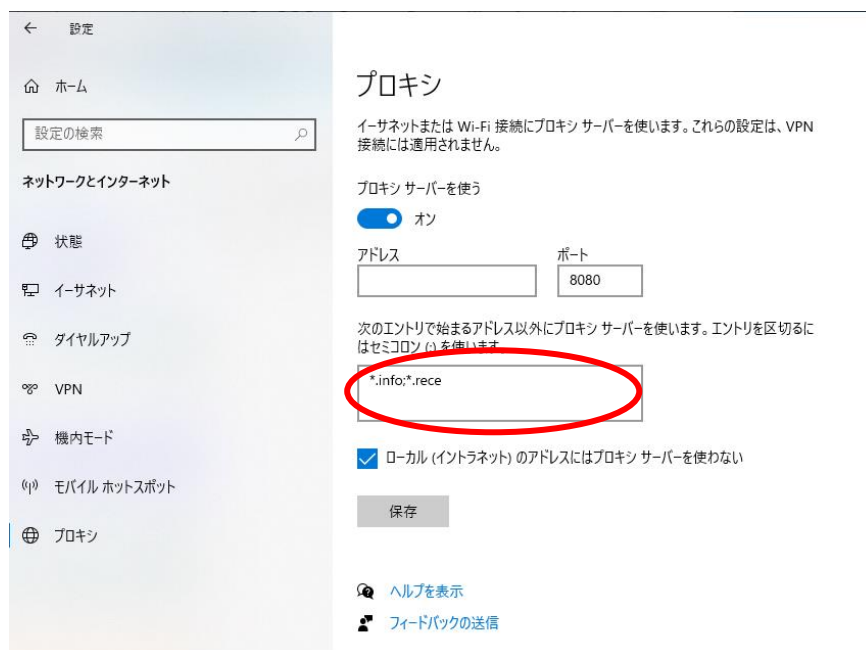
.info;.rece

☒ 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～



～Windows10 の画面～

(4) 以上でプロキシの設定は終了です。

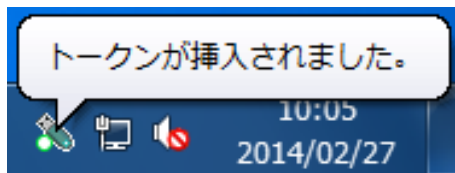
7. VPNの接続方法と切断方法

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

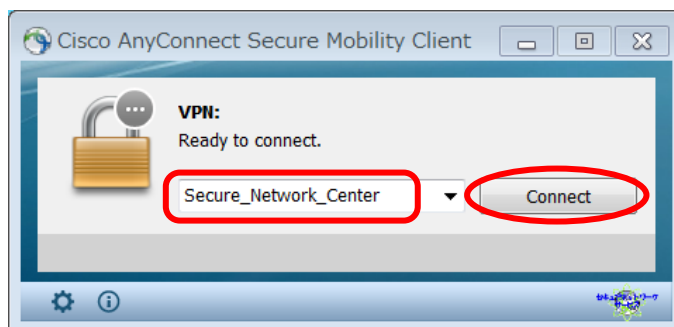
- ① インターネットへ接続します。
- ② USB トークンを USB ポートに挿します。USB トークンが認識されるとタスクバーのアイコンに「トークンが挿入されました。」と表示されます。



- 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。

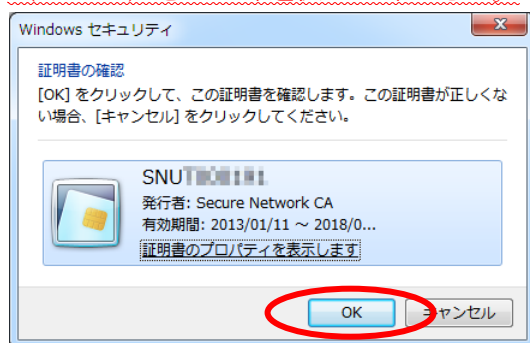


- ④ 入力欄に“Secure_Network_Center”が設定されていることを確認し、[Connect]をクリックします。

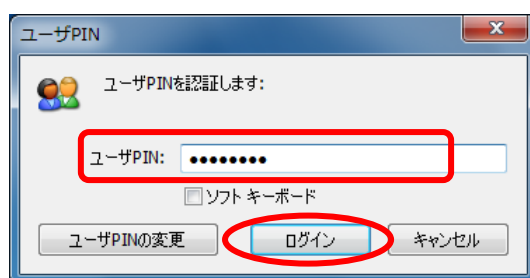


- ⑤ VPN 接続が開始され証明書の確認画面が表示されますので、ユーザ ID を選択し、[OK]をクリックします。

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。



- 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。

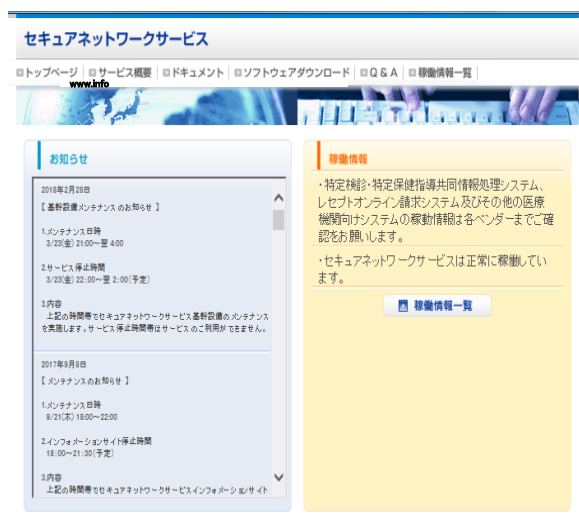


- ⑦ 正しいユーザ PIN (パスワード) を入力すると VPN 接続が確立します。その後 VPN クライアント 2 の画面が自動的に閉じ、タスクバーに青いアイコンが表示されます。



2. セキュアネットワークの接続の確認

- ① 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。



[お気に入り]に追加して
おく事をお勧めします。

- 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。

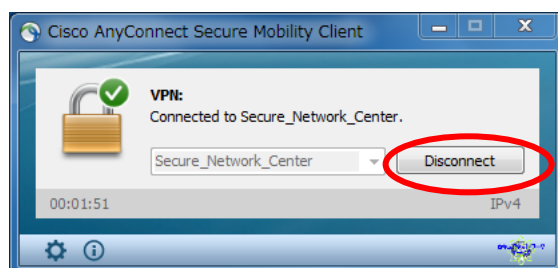
接続方法やご利用方法は各システムのマニュアルをご参照下さい。

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。



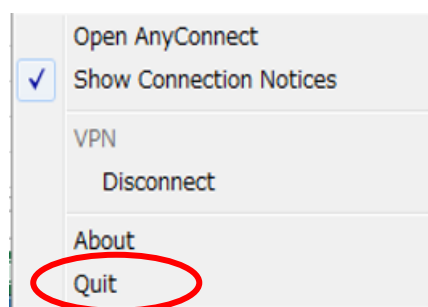
- ② [Disconnect]をクリックします。



- 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。

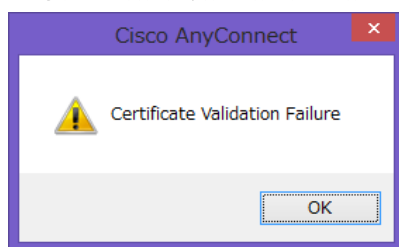


図 8-1

- 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。

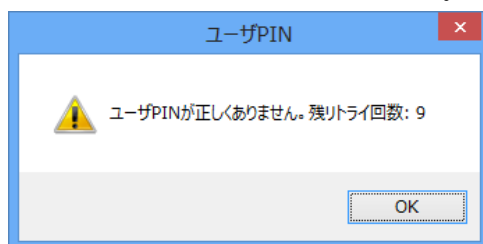


図 8-2

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

注意 : ユーザ P I N 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 P I N はセキュリティ上一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。

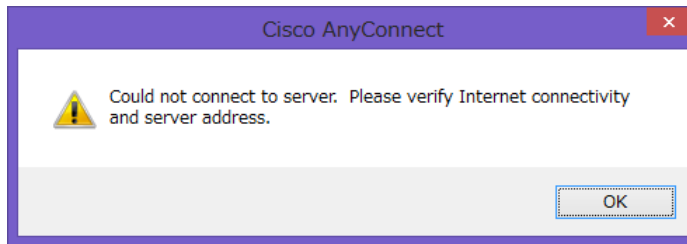


図 8-3

- 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＞

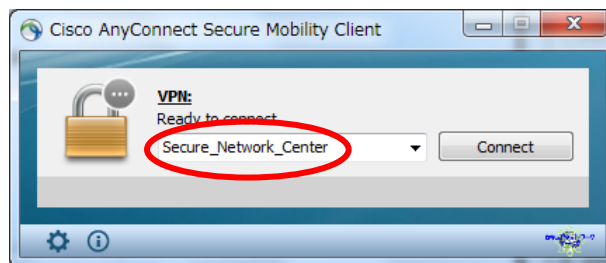
結果 1 : ホームページが表示できない。

インターネットの接続がうまくいっていません。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)



● 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)。

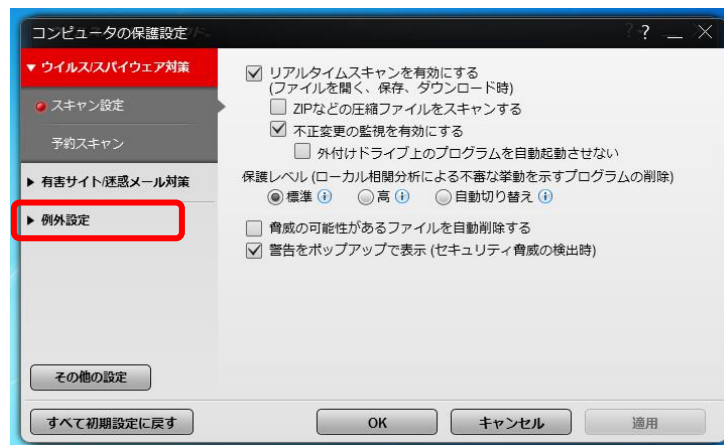
* 以下は主なウイルス対策ソフトの設定をご紹介します。その他の製品も同様の対応が必要となる場合があります。(弊社では個別の製品の対応は致しておりません)

● ウイルスバスタークラウドの設定

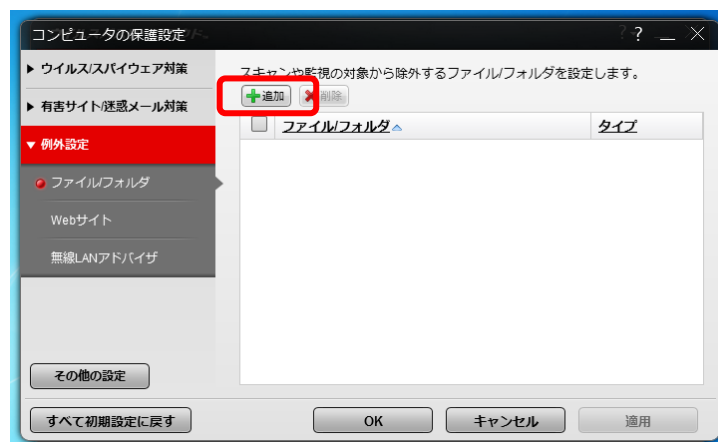
- ① ウイルスバスタークラウドを起動します。
- ② [設定]アイコンをクリックします。



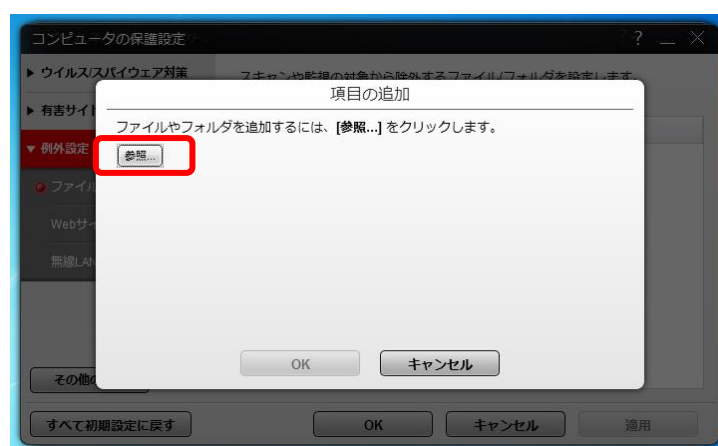
- ③ [例外設定]をクリックします。



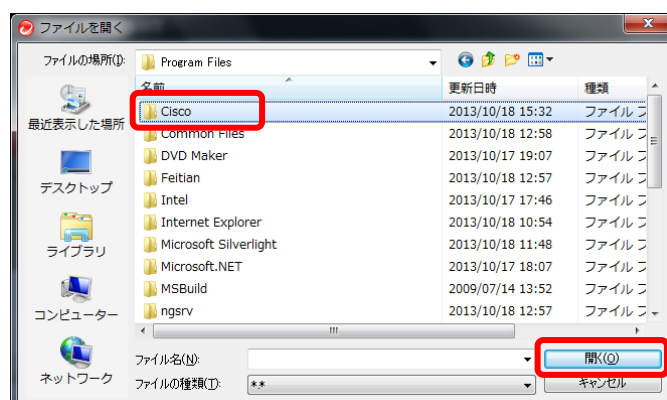
- ④ [追加]をクリックします。



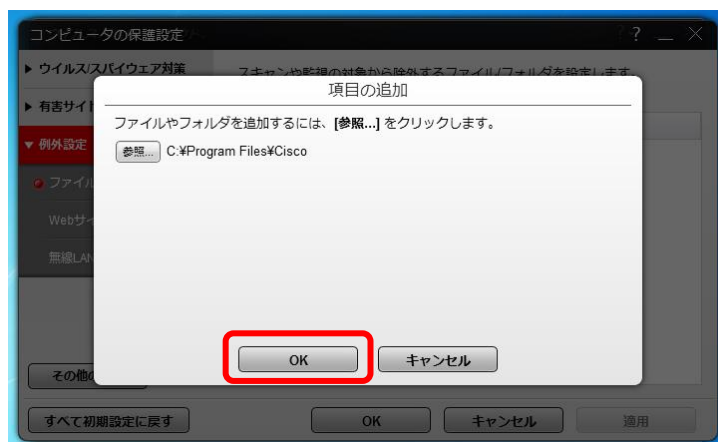
- ⑤ [参照]をクリックします。



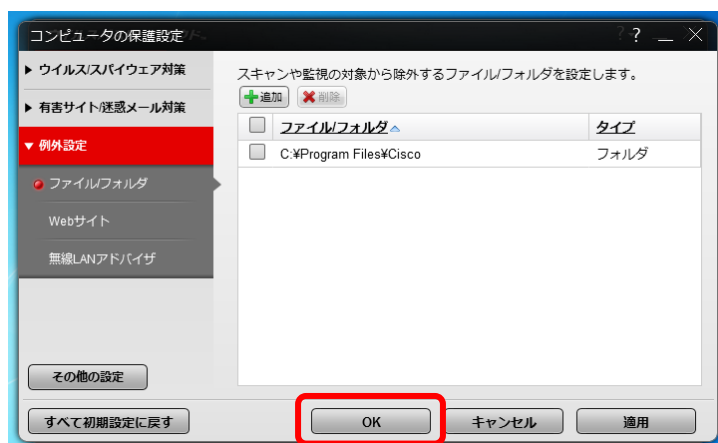
- ⑥ “C:\Program Files\Cisco” を選択し、[開く]をクリックします。



- ⑦ [OK]をクリックします。



- ⑧ [OK]をクリックします。

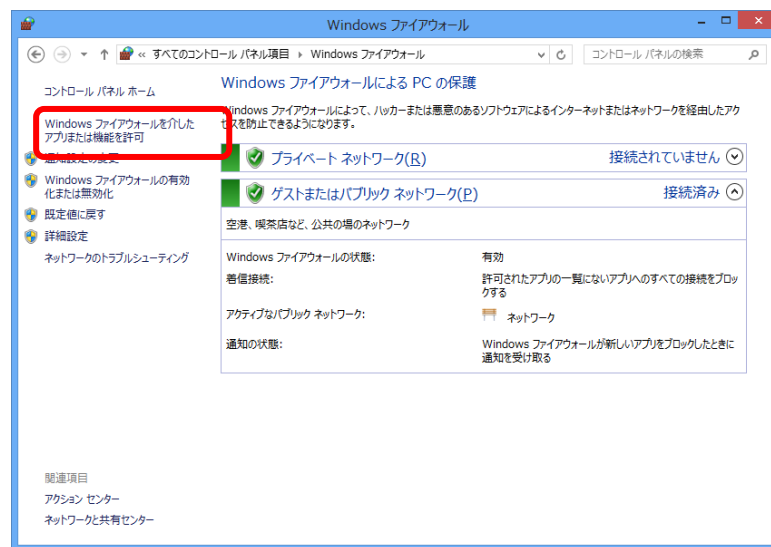


- ⑨ 以上で終了です。

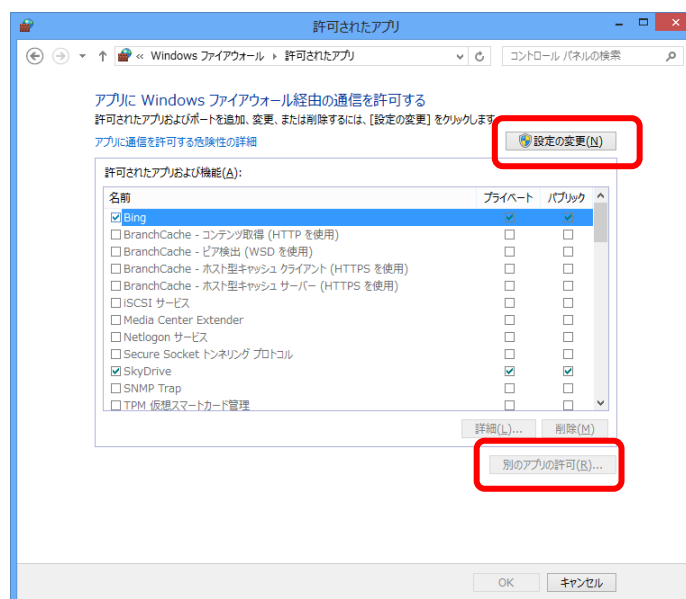
- **Windows ファイアウォールまたはファイアウォールソフトの設定を変更して下さい。(ウイルス対策ソフトの設定は前項をご参照下さい)**

● **Windows 11/10/8.1/8 の Window ファイアウォールの設定**

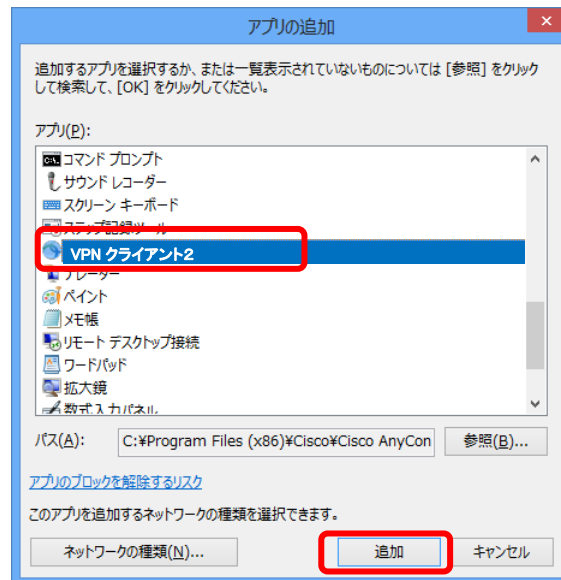
- ① 「設定」→「コントロール パネル」→「Windows ファイアウォール」を開き、「Windows ファイアウォールを介したアプリまたは機能を許可」をクリックします。



- ② 「設定の変更」→「別のプログラムの許可」をクリックします。



- ③ 「VPN クライアント 2」を選択し、[追加]をクリックします。

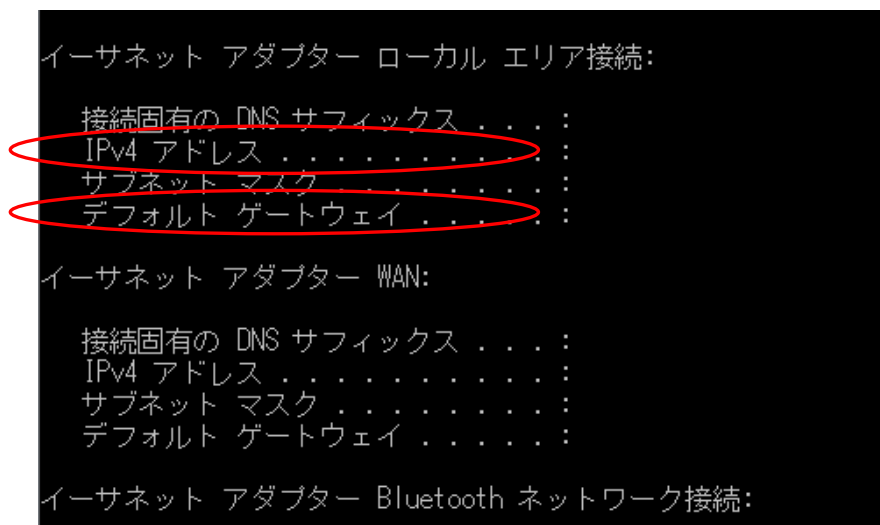


- ④ もう一度、[OK]をクリックして終了です。

- 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。



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

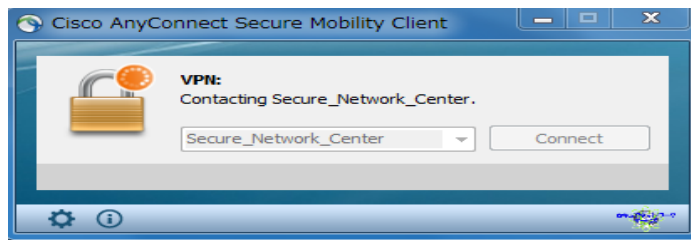


図 8-4

- インターネットが切断されました。インターネット接続状態を確認し再接続して下さい。

- (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。

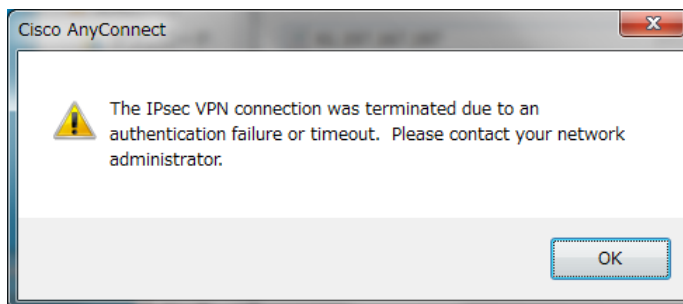


図 8-5

- 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。

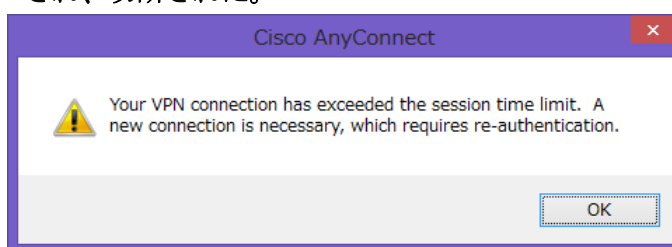


図 8-6

- 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。

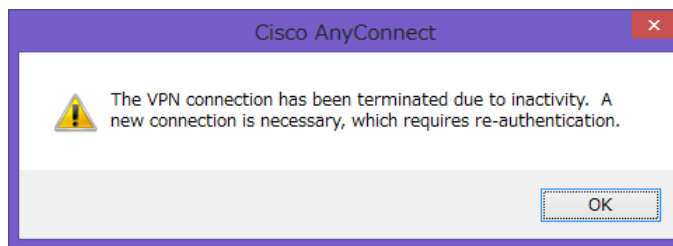


図 8-7

- 規定の無通信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。

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

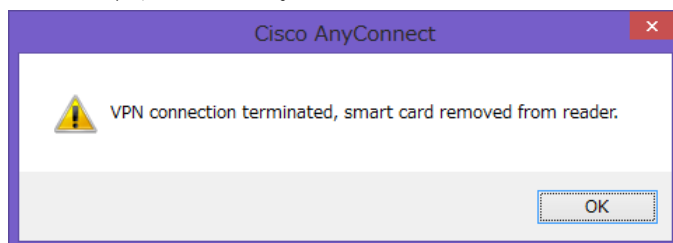


図 8-8

- 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。

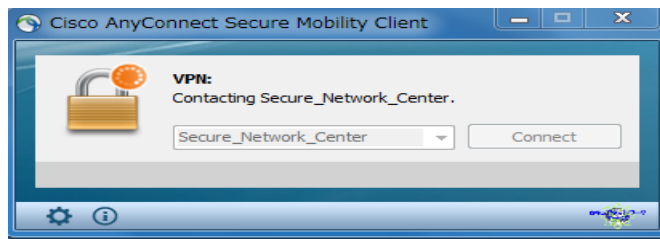
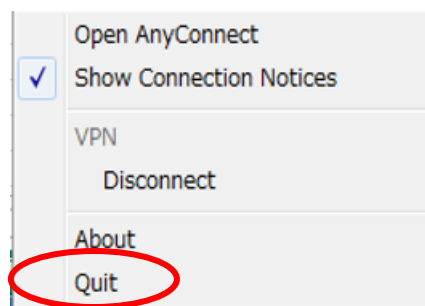


図 8-9

- 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。

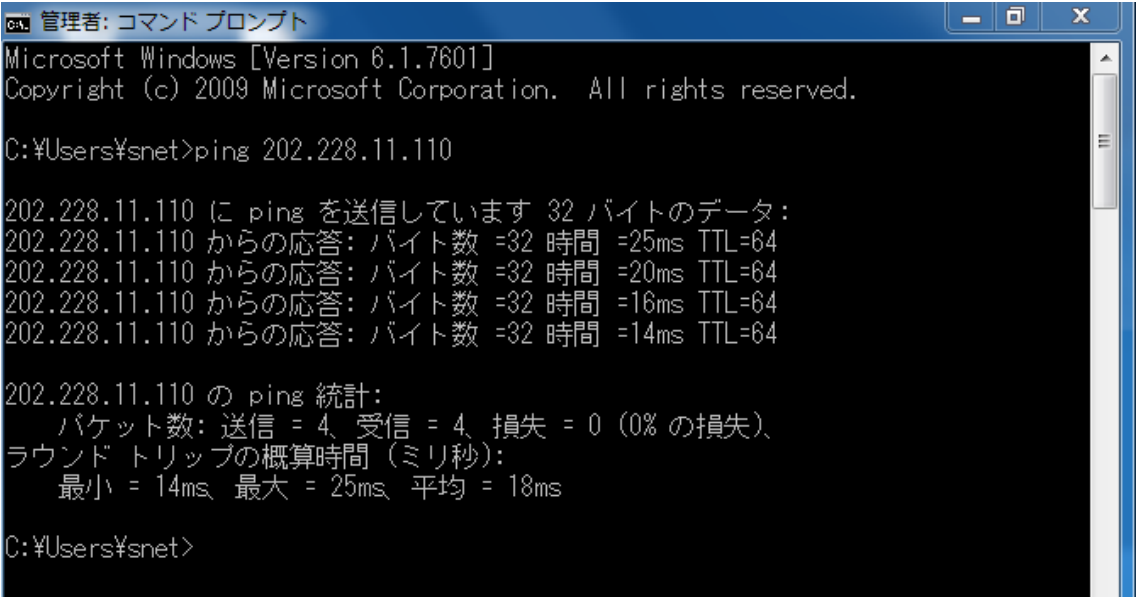
➤ ご利用するサーバに対して通信確認を行なって下さい。

<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
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft 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 =20ms TTL=64
202.228.11.110 からの応答: 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:
    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 = 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

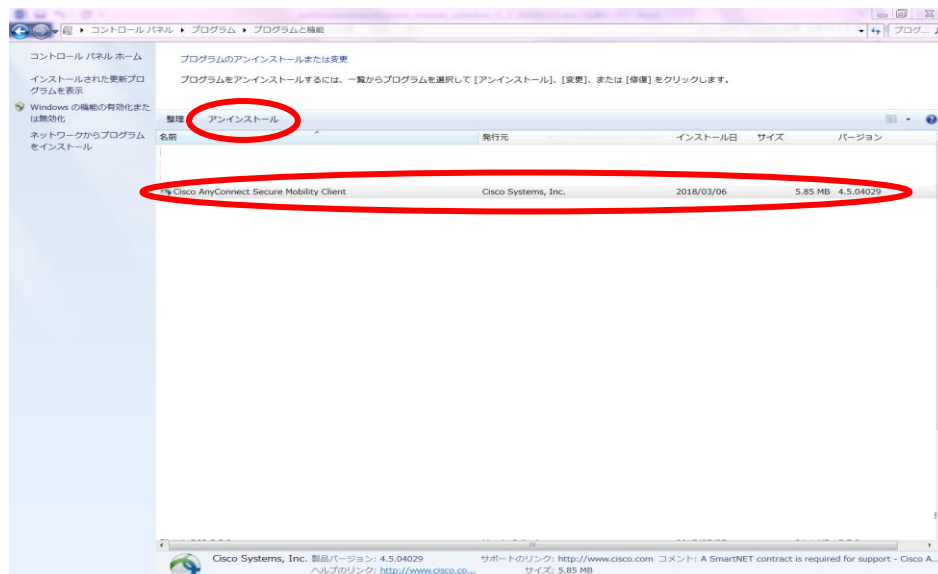
ADSL ルータにブリッジモードの機能がある場合は設定しますと利用可能になる場合があります。ただし、ルータ 1 台につき端末 1 台の利用となります。設定方法は ADSL ルータのマニュアルをご確認下さい。

9. VPNクライアント2のアンインストール

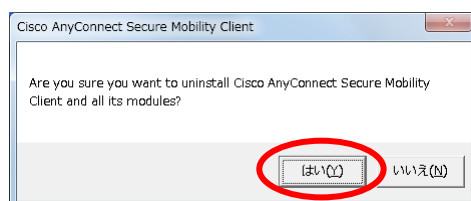
- (1) [スタート]→[コントロールパネル]→[プログラムのアンインストール] の順にクリックして起動します。



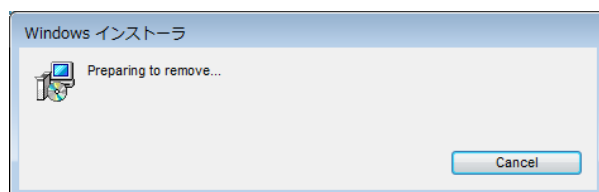
- (2) “Cisco AnyConnect Secure Mobility Client” を選択し、[アンインストール]をクリックします。



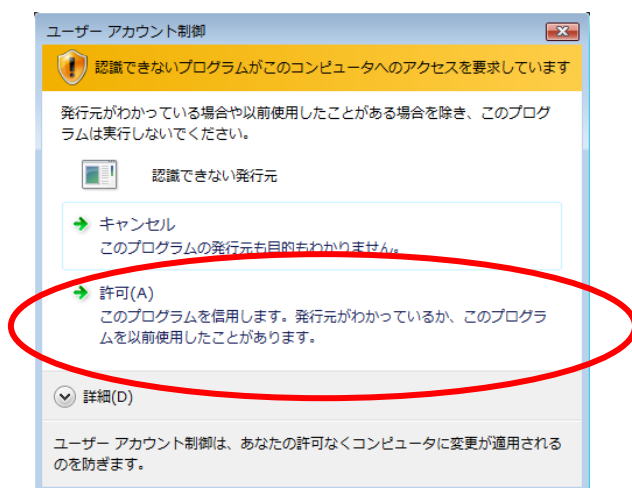
- (3) 確認画面が表示された場合は[はい]をクリックします。



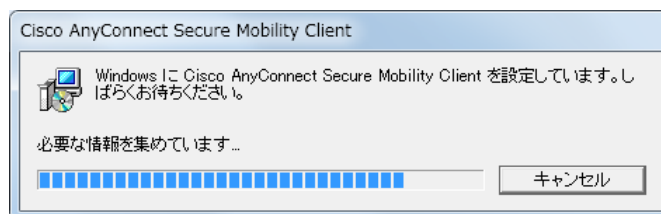
- (4) アンインストールが開始されます。



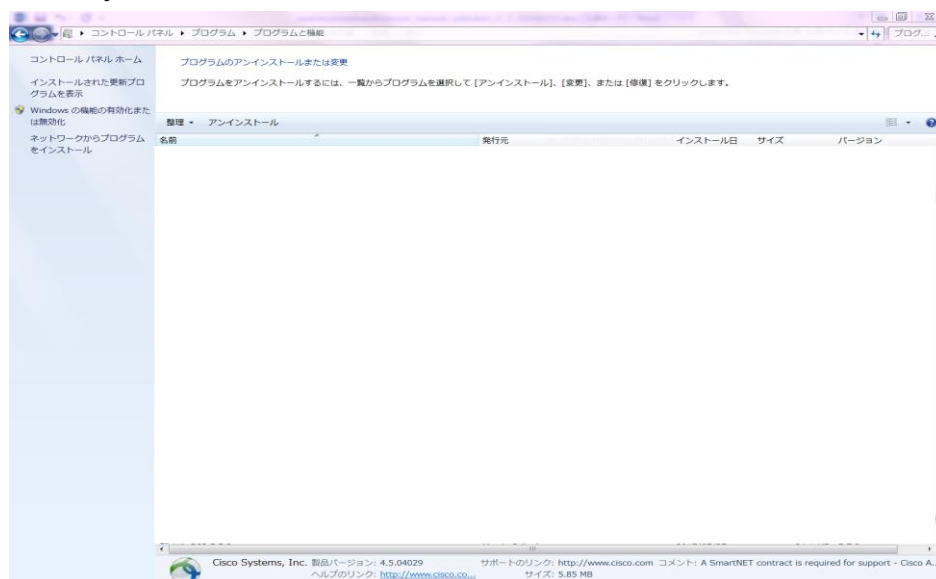
- (5) “ユーザーアカウント制御”が表示された場合は[許可]をクリックします。



- (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。

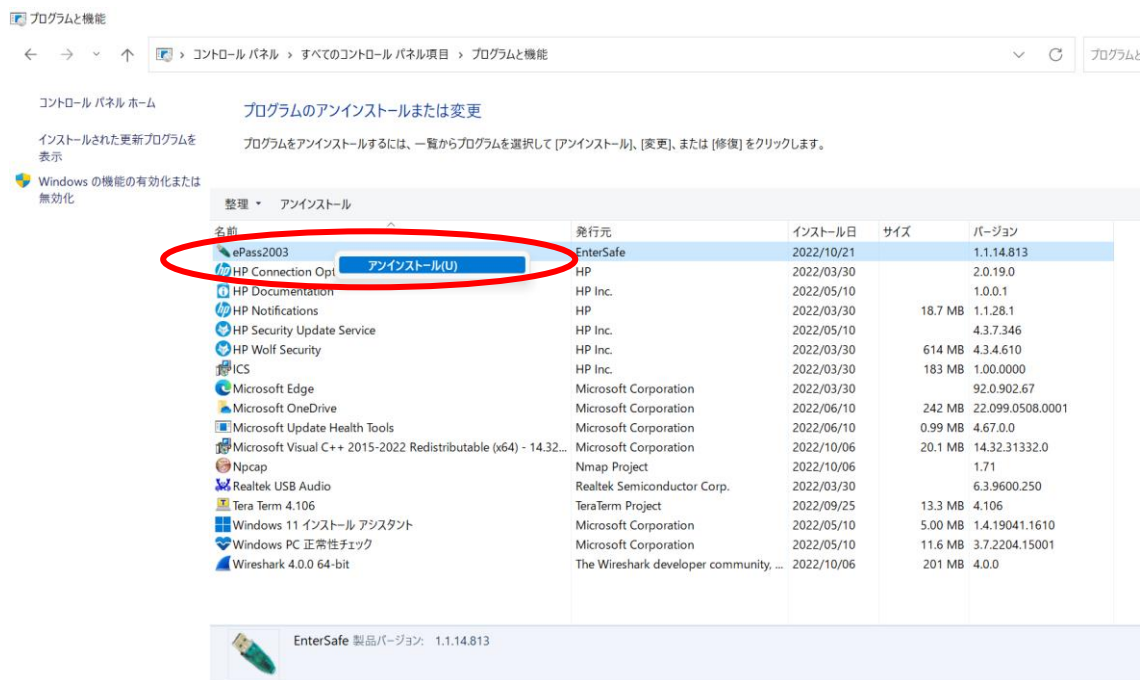


- (9) 以上で VPN クライアント 2 のアンインストールは終了です。

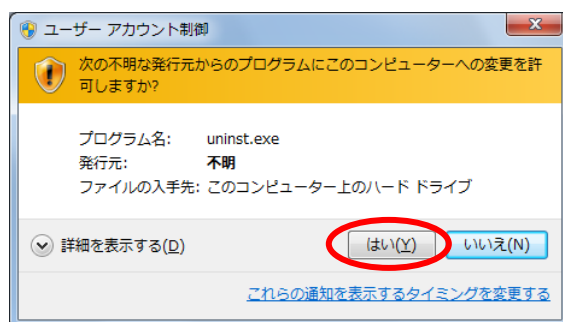
10. USB トークンドライバのアンインストール

- (1) アンインストーラを起動します。

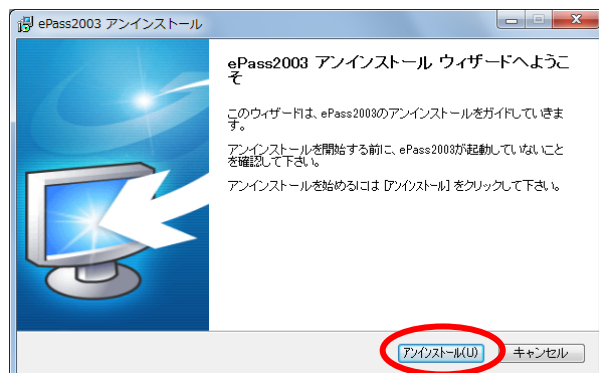
USB トークン (緑) : [スタート]→[コントロールパネル]→[ePass2003]を右クリックし、[アンインストール] の順にクリックして起動します。



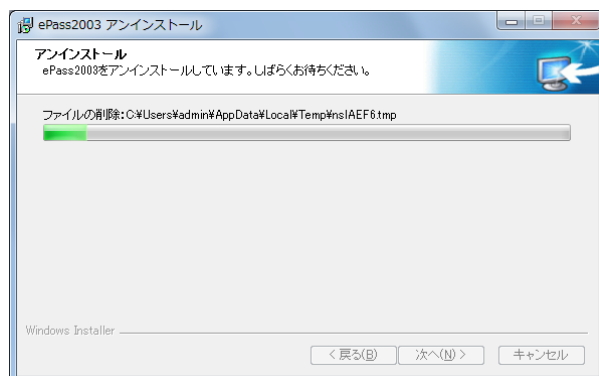
- (2) ユーザーアカウント制御が表示された場合は、[はい]をクリックします。



- (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

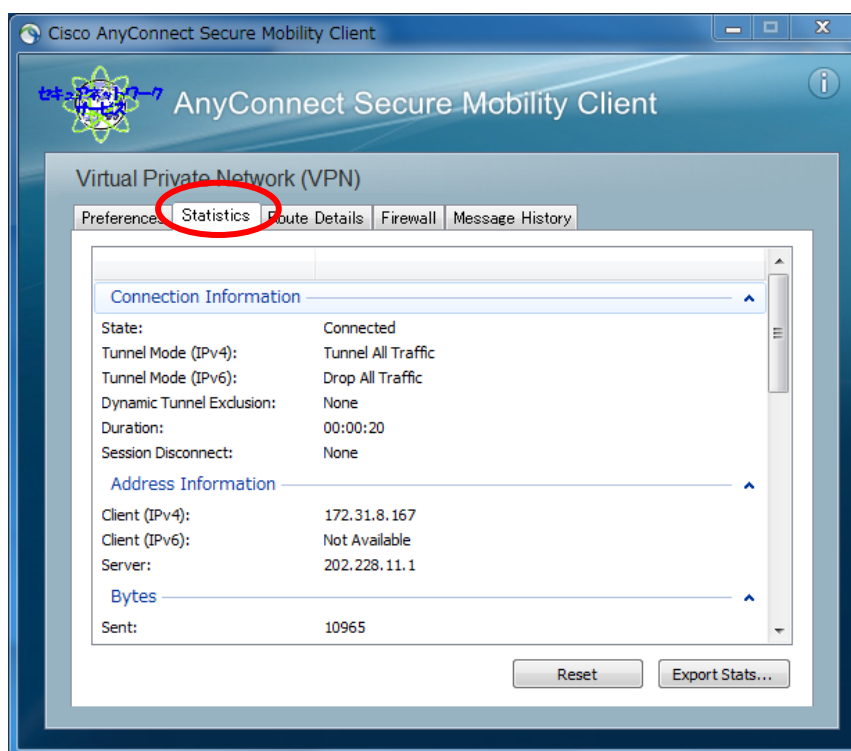
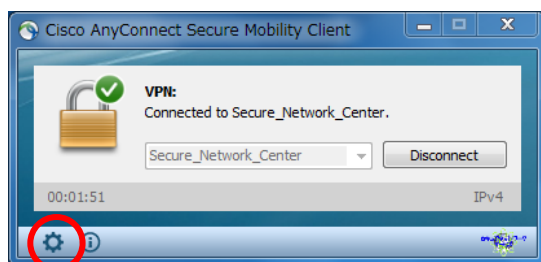
- ① 厚生労働省のガイドラインによりセキュアネットワークサービスではクライアント／サーバ間は HTTP、HTTPS 及び ICMP のみ通信を許可しています。クライアント同士の通信は許可していません。その他の通信ポートをご利用になられる場合やクライアント同士の通信が必要な場合は予めご連絡して頂き個別に対応させていただきます。
- ② セキュアネットワークサービスのご利用中(VPN クライアントソフトの起動中)は、通常のインターネット (Web 閲覧等) 及び社内ネットワーク (ファイルサーバやネットワークプリンタ等) には接続できません。ファイルサーバやネットワークプリンタをご利用になる場合は“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 NAT 環境下であっても非 NAT 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。



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

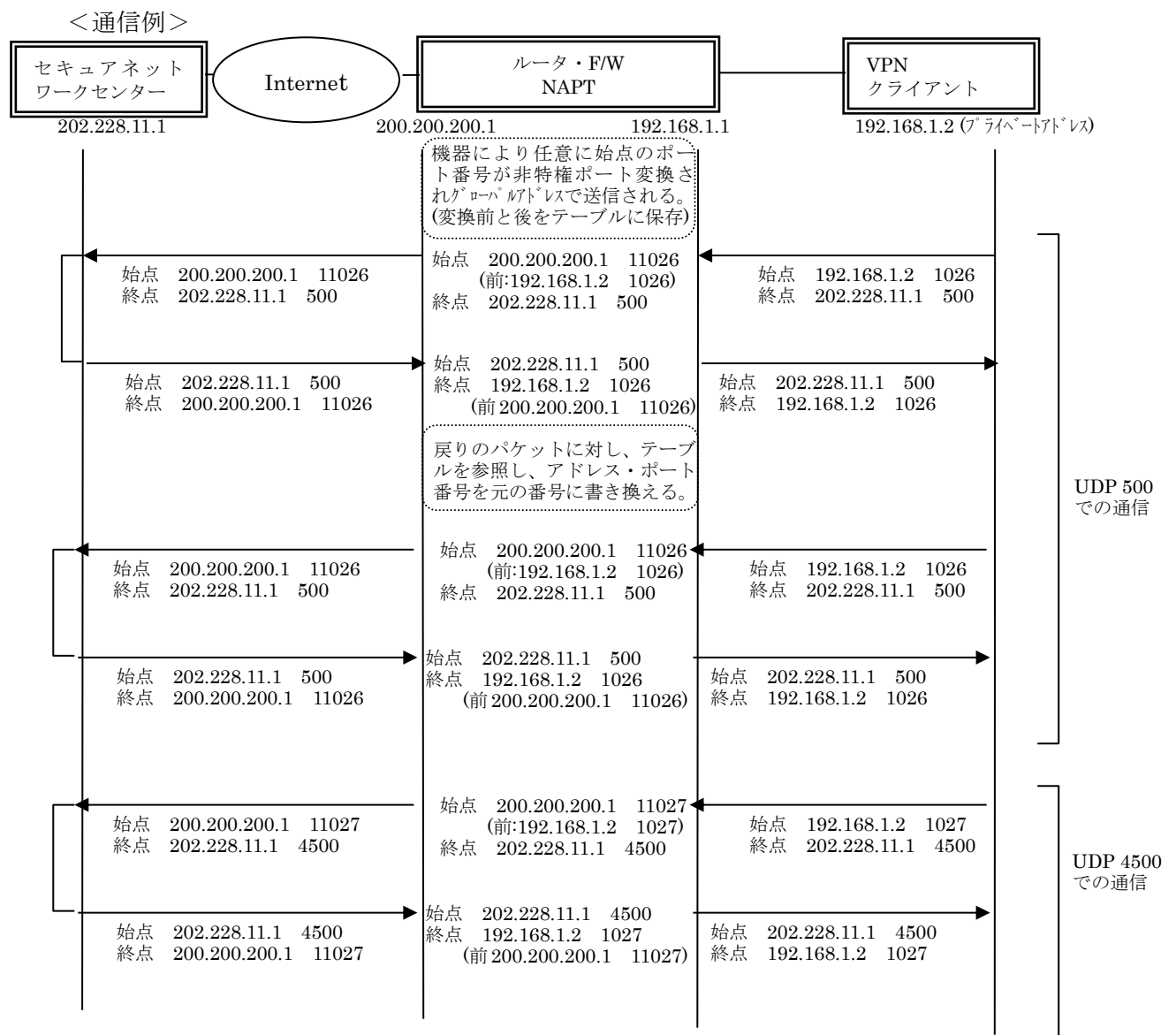
②通信シーケンス

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。



(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/>

以上