

---

---

# SSL-VPN 利用マニュアル

---

---

2024年3月  
第9版

株式会社さくらケーシーエス  
データセンター

## 【目次】

株式会社さくらケーシーエス .....	0
1. はじめに.....	1
2. SSL-VPN サービスご利用の流れ.....	2
2.1. ご利用の流れ.....	2
2.2.1. インターネット環境について .....	2
2.2.2. タイムアウトについて .....	2
2.2.3. プロキシサーバーについて .....	3
2.2.4. 信頼済みサイトの設定 .....	3
3. アプリのダウンロード・インストール .....	5
4. SSL-VPN トンネル接続 .....	7
4.1. 起動方法 .....	7
4.2. 接続準備 .....	7
4.3. 接続方法 .....	9
5. パスワードの変更 .....	10
5.1. パスワード変更手順.....	10
6. 異なるバージョンのアプリを使用する場合.....	14
7. 付録 .....	15
A. プロキシ設定手順.....	15
B. SSL-VPN トンネル接続時 Status のパーセント別エラー対処方法 .....	20
C. インターネット接続確認方法.....	22

# 1. はじめに

本書では下記のサービスで提供している SSL-VPN をご利用いただくための基本的な操作・設定方法について説明しております。

## (1) 対象サービス

- ① さくら UTOPIA クラウド IaaS サービス
- ② さくら UTOPIA クラウド オンラインストレージサービス

## (2) 対象サービスにおいて SSL-VPN が提供される機能

- ① インターネット接続サービス (10M/100M ベストエフォート)
- ② IaaS サービスで提供される管理コンソール「Prism」
- ③ IaaS サービスで提供されるバックアップオプションの管理コンソール

### 本書内の表記法について

本書では以下の表記法を使用しております。

下線 … 操作の際に実際に入力する項目を意味します。

[ ] … 操作の際にクリックするリンク・ボタンを意味します。

「 」 … 本書に記載されている別章を意味します。また、画面名やダイアログ名、参照する場所などを示す場合も鍵カッコ (「 」) で囲んであらわします。

## 2. SSL-VPN サービスご利用の流れ

### 2.1. ご利用の流れ

SSL-VPN サービスをご利用になる際の手順は、以下のようになります。

ステップ	内容
1. 事前準備	サービスご利用開始時にお渡ししております、以下の書類をご準備下さい。 <ul style="list-style-type: none"><li>• 操作画面情報…IaaS サービスで管理者が使用するサイトアクセス情報が記載されています。</li><li>• SSL-VPN 設定情報…利用者が SSL-VPN トンネル接続に必要な URL・ユーザー名・パスワードとパスワード変更ページの URL が記載されています。</li><li>• SSL-VPN ユーザー名・パスワード一覧…利用者が SSL-VPN トンネル接続に必要な URL・ユーザー名・パスワードとパスワード変更ページの URL が記載されています。</li></ul>
2. アプリのダウンロード・インストール	SSL-VPN トンネル接続に必要なアプリをダウンロードし、インストールします。詳細は「3. アプリのダウンロード・インストール」をご参照ください。
3. SSL-VPN トンネル接続	アプリを利用し、WEB 操作画面やご利用サーバーまでの仮想ネットワーク接続を行います。詳細は「4. SSL-VPN トンネル接続」をご参照ください。 また、使用する ID のパスワードを変更することができます。詳細は「5. パスワードの変更」をご参照ください。

#### 2.2.1. インターネット環境について

SSL-VPN をご利用いただく為には、インターネットに接続できる環境が必要です。

また、インターネットに対して以下のポート番号が利用できる必要がありますので、ファイアウォール等で遮断している場合はご利用のファイアウォール等の設定変更が必要です。

##### ■ 必要なポート

TCP：弊社が指定するポート番号（端末から SSL-VPN アクセスサイトへの通信）

ポート番号については、ご利用開始時に提供する資料に記載しています。

ファイアウォール等の設定が正しく設定されているか確認する場合、「7. 付録 C. インターネット接続確認方法」をご参照ください。

#### 2.2.2. タイムアウトについて

ログイン後『**240 分**』を超過しますと、自動でログアウトします。（SSL-VPN トンネル接続も切断されます）。

### 2.2.3. プロキシサーバーについて

インターネット接続時にプロキシサーバーをご利用の場合は、「7.付録 A.プロキシ設定手順」を参照し、設定を行ってください。

### 2.2.4. 信頼済みサイトの設定

ブラウザのセキュリティレベルについて、「信頼済みサイト」ゾーンに SSL-VPN アクセスサイトの URL を追加する設定が必要になる場合があります。

- ① 左下のスタートボタンをクリックし、[Windows システム ツール] – [コントロールパネル]をクリックします。

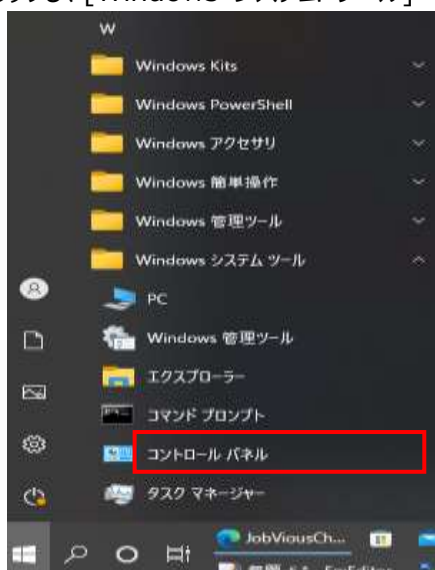


図 2.2.4.1 信頼済みサイトの設定 (1)

- ② [インターネット オプション]をクリックします。



図 2.2.4.1 信頼済みサイトの設定 (2)

- ③ 「インターネットオプション」画面が表示されたら、「セキュリティ」タブをクリックします。

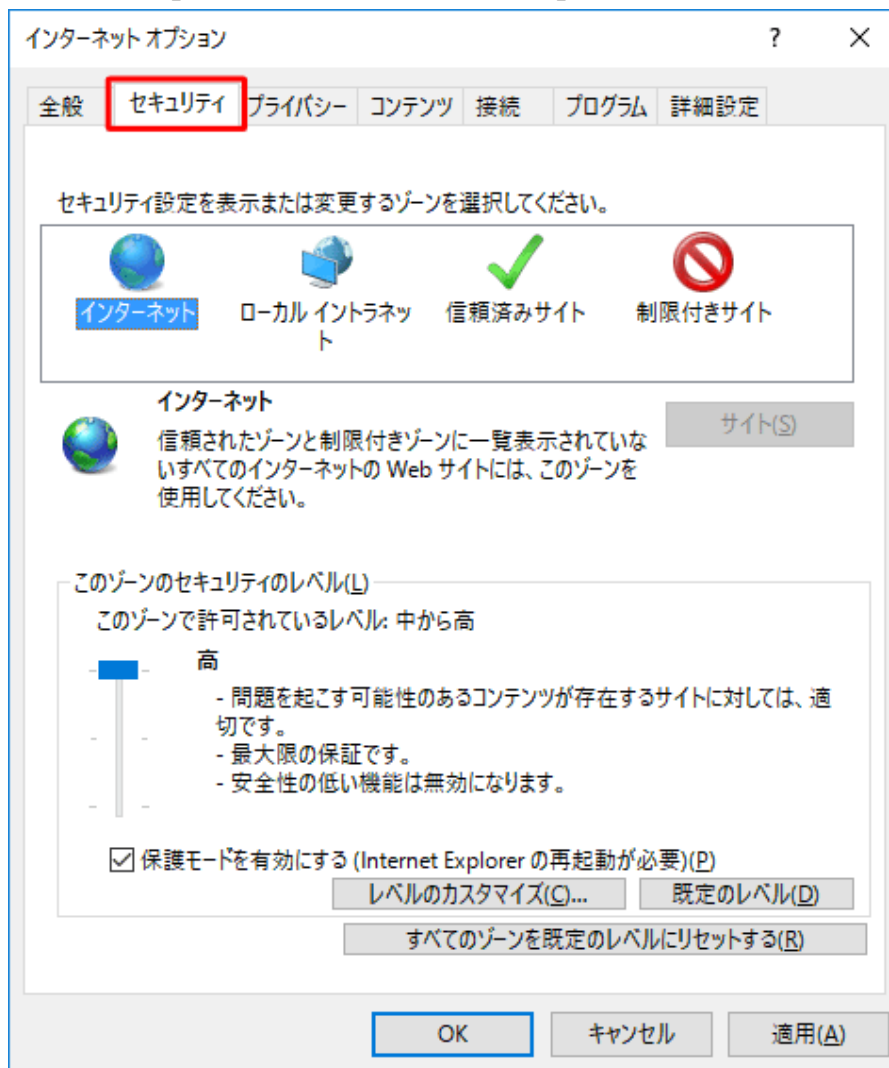


図 2.2.4.3 信頼済みサイトの設定 (3)

- ④ 「信頼済みサイト」ゾーンに弊社 SSL-VPN アクセスサイトの URL を入力します。  
「 https://xxx.xxx.xxx.xxx:弊社が指定するポート番号」の IP アドレス部分「xxx.xxx.xxx.xxx」を入力し、[追加]ボタンをクリックします。「追加」をクリックすることで、信頼済みサイトに登録されます。[閉じる]ボタンをクリックします。

### 3. アプリのダウンロード・インストール

SSL-VPN 接続をするために必要なアプリをダウンロードし、インストールします。

既に Forticlient SSL-VPN がインストールされている場合は「6.異なるバージョンのアプリを使用する場合」をご確認ください。

- ① ブラウザで下記 URL にアクセスし、SSL-VPN アプリケーション（FortiClient）から zip ファイルをダウンロードします。

<https://www.kcs.co.jp/ja/service/utopia/download.html>

- ② ダウンロードしたファイルを解凍します。  
解凍する際に必要なパスワードは「SKCSVPN」です。

- ③ ご利用 PC のバージョンに合わせて、アプリを実行します。

\* アプリのインストールには、管理者権限での実行が必要です。

\* 弊社にてメンテナンス終了後に再度、アプリの再インストールが必要になる場合があります。

ご利用 PC の OS が「Windows10」以降の WindowsPC の場合	“sslvpnclient_2331.exe”を実行します。
ご利用 PC の OS が「Windows10」より古い WindowsPC の場合	“sslvpnclient_2317.exe”を実行します。

- ④ セキュリティの警告にて、[実行する]をクリックします。



図 3.1 セキュリティの警告④

- ⑤ インストーラが起動します。お使いの環境によっては、以下の画面が表示されます。その場合[Run as administrator]をクリックします。

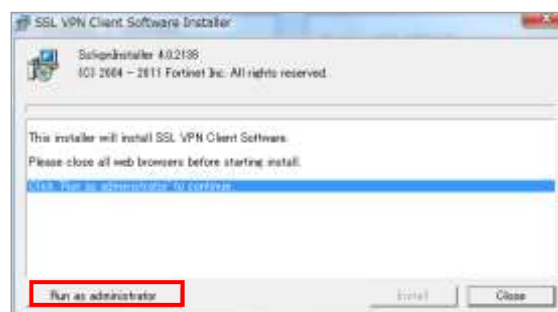


図 3.2 インストーラ④

- ⑥ ユーザーアカウント制御の画面が表示された場合は、[はい]をクリックします。

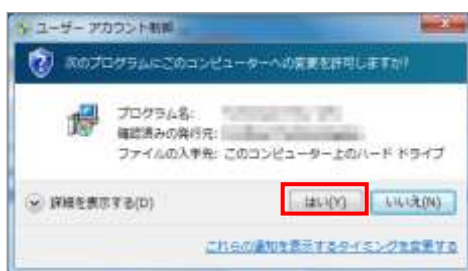


図 3.3 ユーザーアカウント制御

- ⑦ [Install]をクリックします。

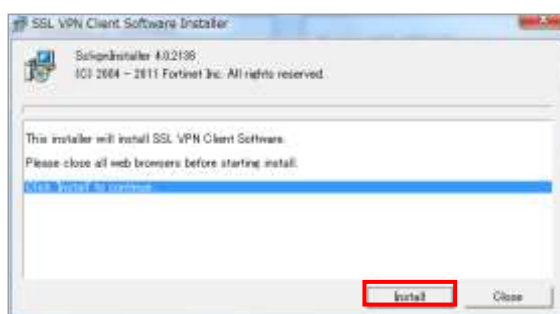


図 3.4 インストーラ②

- ⑧ インストールが実行されます。“Done!”のメッセージ表示後、[Close]をクリックします。



図 3.5 インストーラ③



## 4. SSL-VPN トンネル接続

### 4.1.起動方法

スタートメニューにある“FortiClient SSLVPN”を**管理者権限で起動（アイコンを右クリックして[その他]-[管理者権限として実行]）**します。



図 4.1 アプリの実行

### 4.2.接続準備

- ① 左下にある[Settings]をクリックします。



図 4.2.1 アプリ設定画面①

- ② 右上にある[New Connection]をクリックします。

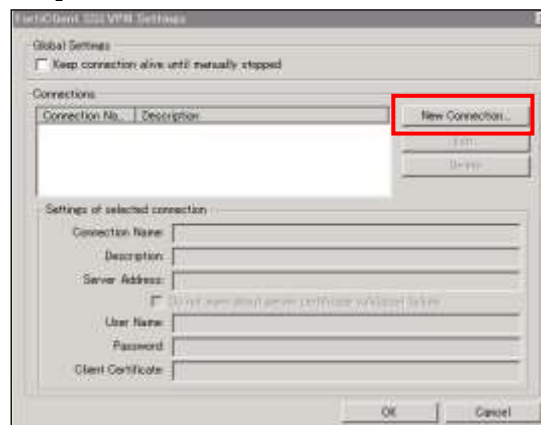


図 4.2.2 アプリ設定画面②

- ③ [Connection Name]に任意の名前を入力、[Server Address]はご利用機能に応じて URL を入力し、[OK]をクリックします。

ご利用機能	[Server Address]に入力する URL
IaaS サービスにてインターネット経由で仮想マシンにアクセスする。	“SSL-VPN 設定情報”に記載されているログインページ URL を入力します。
オンラインストレージサービスにてインターネット経由でボリュームにアクセスする。	“SSL-VPN 設定情報”に記載されているログインページ URL を入力します。
IaaS サービスでバックアップサービス管理コンソールにアクセスする。	“バックアップサービス 設定情報”に記載されているバックアップサービス接続用 SSL-VPN 設定情報の URL を入力します。
IaaS サービスで WEB 操作画面・バックアップ・リストア操作画面にアクセスする。	“操作画面情報”に記載されているサイトアクセス情報の URL を入力します。

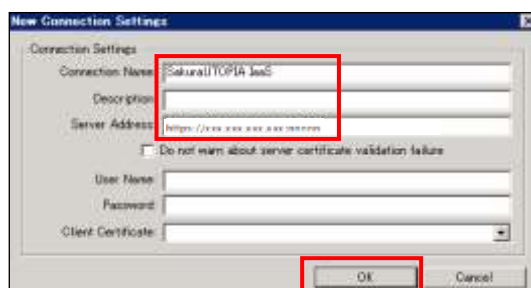


図 4.2.3 アプリ設定画面③

※[Server Address]部分について、ポート番号の最後を「: 弊社が指定するポート番号/」と入力した場合、エラーになる場合があります。

この場合は最後の「/」を削除し、「: 弊社が指定するポート番号」で終わるように入力してください。

- ④ [OK]をクリックします。

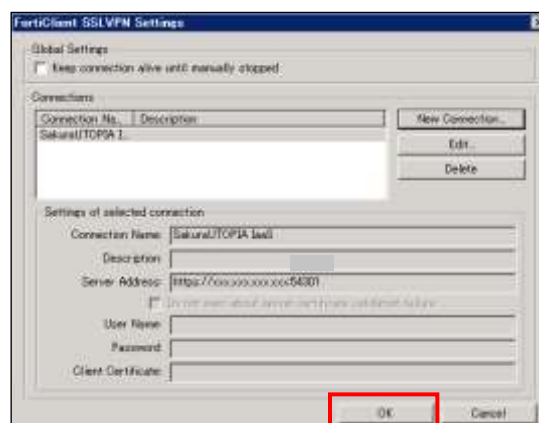


図 4.2.4 アプリ設定画面④

### 4.3.接続方法

- ① [Connection Name]で先程作成した設定を選択し、“Username”、“Password”を入力し、[Connect]をクリックします。

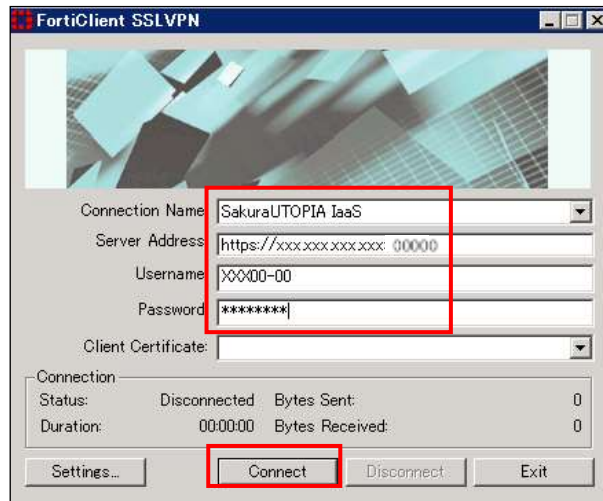


図 4.3.1 アプリ接続画面①

- ② Connection のステータスが“Connecting...(40)”になるとセキュリティの警告画面が表示される場合があります。この場合は[はい]をクリックします。

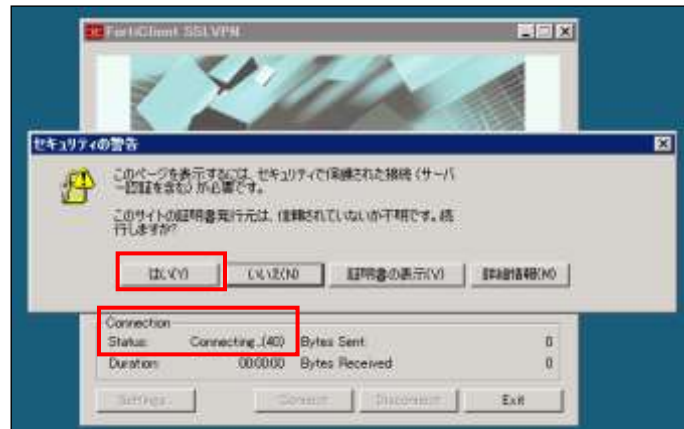


図 4.3.2 アプリ接続画面②

- ③ Connection のステータスが“Connected”になると接続完了です。切断する場合は[Disconnected]をクリックします。

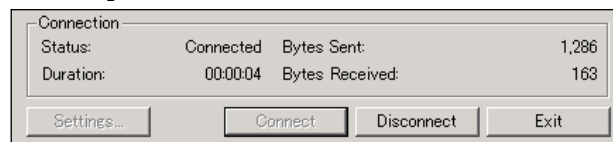


図 4.3.3 アプリ接続画面③

- ④ Connection のステータスが“Connected”にならない場合、「7.付録 B. SSL-VPN トンネル接続時 Status のパーセント別エラー対処方法」をご確認ください。

## 5. パスワードの変更

### 5.1.パスワード変更手順

ログイン時に使用するパスワードは、ご利用のユーザー自身にて変更することが可能です。  
変更手順は以下のとおりです。

- ① SSL-VPN トンネル接続を行います。
- ② Web ブラウザを起動し、“お客様設定情報”に記載しているパスワード変更用 URL へアクセスします。  
※下記のようなプライバシーの警告が表示された場合は、[詳細設定]をクリックし、  
[xxx.xxx.xxx.xxx にアクセスする（安全ではありません）]をクリックして下さい。  
※ブラウザにより表示内容が異なります。



図 5.1.0.1 ログインページ①

- ③ ログイン画面が表示されますので、“お客様設定情報”に記載している“ユーザー名”と“パスワード”を“ログイン名”、“パスワード”に入力し、[ログイン]をクリックします。

※2024/3/29 より URL が変更になりました。ご注意ください。

変更前の URL <http://【パスワード変更用 URL】/user>

変更後の URL <https://【パスワード変更用 URL】>

図 5.1.0.2 ログイン変更ページ②

- ④ 以下のようなページが表示されます。右上の人のマークから[パスワードの変更]をクリックします。



図 5.1.1 パスワード変更ページ①

- ⑤ 各項目を入力し、[OK]をクリックします。

図 5.1.2 パスワード変更ページ②

- [現在のパスワード]にパスワードを変更したいユーザーの現在のパスワードを入力してください。
- [新しいパスワード]、[新しいパスワード（確認）]に変更するパスワードを入力してください。
- 各パスワード欄への入力時には、入力した内容が“\*”や“●”等の伏せ字で表示されます。パスワードの大文字や小文字、キーボード上の Num Lock キー、Caps Lock キーの ON / OFF に注意して入力してください。
- 新しく設定するパスワードは、下表の規則を満たしている必要があります。

パスワード長	最低 8 文字（最大 253 文字）
使用可能文字	半角英小文字：abcdefghijklmnopqrstuvwxyz 半角英大文字：ABCDEFGHIJKLMNOPQRSTUVWXYZ 半角数字：0123456789 半角記号：`~!@#\$%^&*()-_=[\]{};:“,./?
文字種の組み合わせ（複雑性）	英大文字、英小文字、数字の 3 種のうち、2 種以上を使用しているか、または記号を使用している必要があります
同一パスワードの使用	現在と同じパスワードは設定できません 過去 2 世代と同じパスワードは設定できません

表 5.1.1 パスワード設定ルール

- ⑥ 以下の画面が表示されれば、変更完了です。[×]をクリックし、右上の人のマークから[ログアウト]をクリックして、Web ブラウザを終了します。（変更したパスワードは即時有効となります）



図 5.1.3 パスワード変更完了①



図 5.1.4 パスワード変更完了②

パスワード変更に失敗した場合、以下のようなエラーが表示されます。  
[OK]をクリックし、再度変更をやり直してください。

- 現在のパスワードが間違っています
- パスワードが一致していません。
- パスワードの長さが足りません。
- 使用できない文字が含まれています。
- 複雑さの要件を満たしていません。
- 現在と同じパスワードです。
- 最近使用されたパスワードです。

## 6. 異なるバージョンのアプリを使用する場合

弊社が提供していますアプリと異なるバージョンのアプリを使用しても SSL-VPN 機能が利用できる場合がありますが、本サービスのサポート外となります。

異なるバージョンのアプリを使用する場合はお客様の自己責任にてご使用ください。

設定方法につきましても使用するアプリのマニュアルをご確認ください。

VPN接続の編集

VPN: SSL-VPN | IPsec VPN | XMIP

接続名: SakuraUTOPIA IaaS

説明: SakuraUTOPIA IaaS

リモートGW: XXX.XXX.XXX.XXX ✖  
+リモートゲートウェイを追加

ポートの複製: 00000

Enable Single Sign On (SSO) for VPN Tunnel

クライアント証明書: なし

認証:  ユーザ名入力  ユーザ名を保存

無効なサーバ(証明書の警告を非表示)

キャンセル 保存

図 6.1 [参考]異なるバージョンのアプリの設定例



## 7. 付録

### A. プロキシ設定手順

インターネット接続時に、プロキシサーバーを使用している場合、以下の設定をして頂くことでインターネットと、SSL-VPN トンネル接続の同時利用が可能となります。

(該当されない環境でご利用の方は、以下の作業は不要です)

- ① 左下のスタートボタンをクリックし、[Windows システム ツール] – [コントロールパネル]をクリックします。

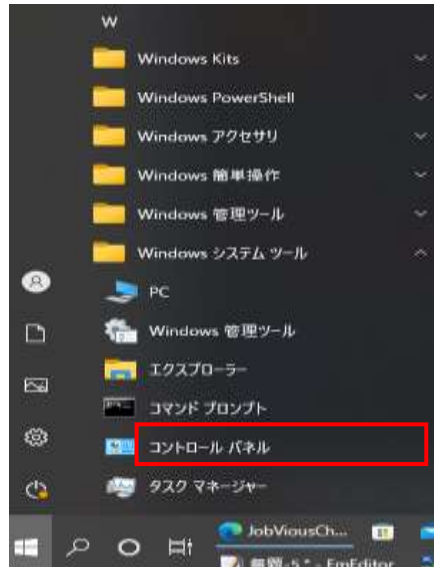


図 7.A.1 プロキシ設定 (1)

- ② [インターネット オプション]をクリックします。



図 7.A.2 プロキシ設定 (2)

- ③ [接続]タブの[ダイヤルアップと仮想プライベート ネットワークの設定]から、[fortissl]の接続を選択し、[設定]ボタンをクリックします。

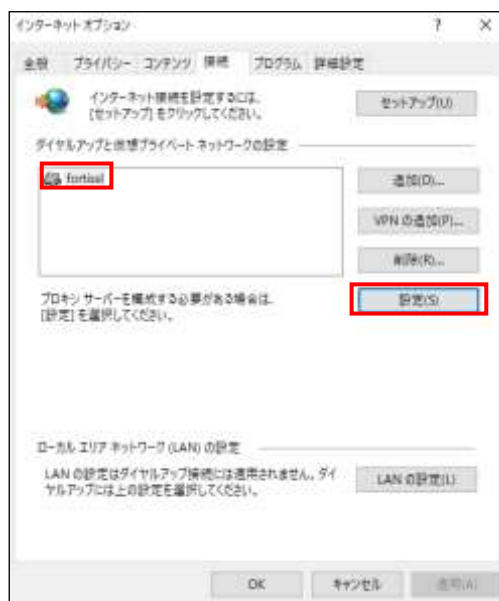


図 7.A.3 インターネットオプション 接続タブ

- ④ [fortissl の設定]画面にて、ご利用環境のプロキシサーバー設定を入力し、[詳細設定]ボタンをクリックします。

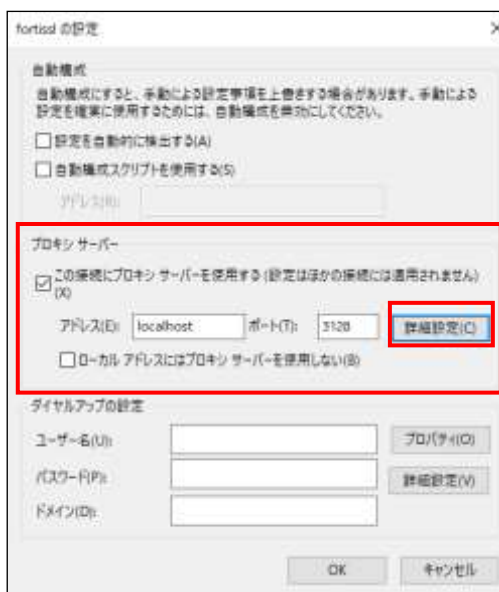


図 7.A.4 fortissl の設定

- ⑤ [例外]にトンネル接続後にアクセスする URL を入力し、[OK]ボタンをクリックします。

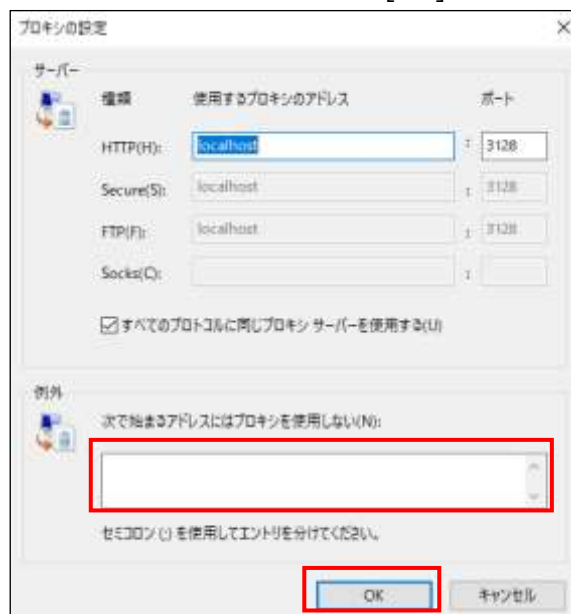


図 7.A.5 プロキシの例外設定

IaaS サービスの 管理者の場合	ssp-vpn.sakura-utopia.jp; backup-vpn.sakura-utopia.jp;パスワード変更ページ の IP アドレス;ご利用サーバーの IP アドレス
上記以外の場合	パスワード変更ページの IP アドレス;ご利用サーバーの IP アドレス

表 7.A.1 サービス別 例外設定する URL

- ⑥ プロキシサーバーで自動構成をご利用の場合、ご利用環境のプロキシサーバー設定を入力し、プロキシサーバー管理者様に「表 7.A.1 サービス別 例外設定する URL」の例外設定をご依頼ください。

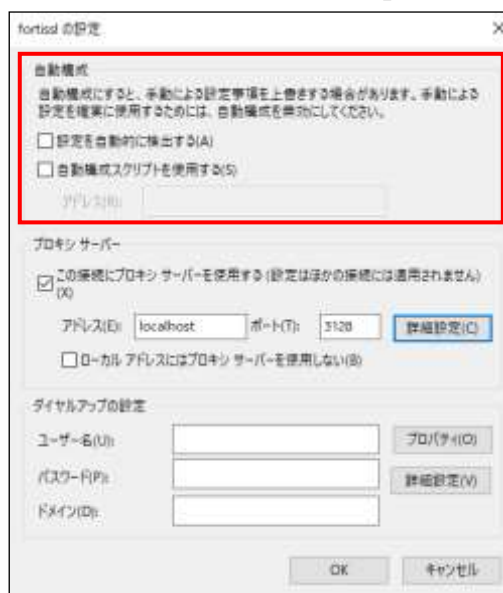


図 7.A.6 fortissl の設定

- ⑦ [OK]ボタンをクリックし、[インターネット オプション]を閉じます。

- ⑧ トンネル接続後、ブラウザでご利用サーバーにアクセスする場合はブラウザのプロキシ設定が必要です。

Chrome の場合、左下のスタートボタンを右クリックし、[システム]をクリックします。



図 7.A.8 プロキシ設定 (3)

- ⑨ 左上の[設定の検索]に“プロキシ”と入力し、[プロキシの設定]をクリックします。

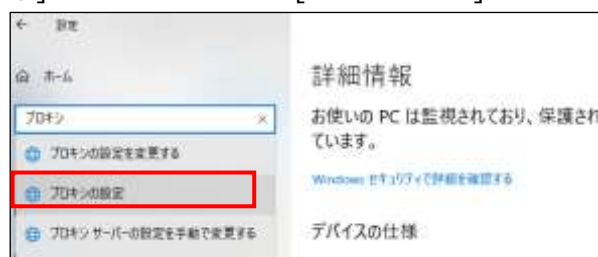


図 7.A.9 プロキシ設定 (4)

- ⑩ 以下の画面が表示されます。



図 7.A.10 プロキシ設定 (5)

- ⑪ 手動プロキシ セットアップに、ご利用環境のプロキシサーバー設定を入力し、[例外]にトンネル接続後にアクセスする URL を入力し、[保存]ボタンをクリックします。

図 7.A.11 手動プロキシ セットアップ

IaaS サービスの 管理者の場合	ssp-vpn.sakura-utopia.jp; backup-vpn.sakura-utopia.jp;パスワード変更ページの IP アドレス;ご利用サーバーの IP アドレス
上記以外の場合	パスワード変更ページの IP アドレス;ご利用サーバーの IP アドレス

表 7.A.2 サービス別 例外設定する URL (表 7.A.1 と同一)

- ⑫ プロキシサーバーで自動構成をご利用の場合、自動プロキシ セットアップご利用環境のプロキシサーバー設定を入力し、プロキシサーバー管理者様に「表 7.A.1 サービス別 例外設定する URL」の例外設定をご依頼ください。

図 7.A.12 自動プロキシ セットアップ

## B.SSL-VPN トンネル接続時 Status のパーセント別エラー対処方法

SSL-VPN トンネル接続のため、Forticlient を実行したが接続できない（Connecting（XX）の後 Disconnect になった）場合の対処方法について説明します。

パーセント	原因	対処方法
10%	URL にアクセスできない	URL に誤りが無いかご確認ください。 ・「2.2.1. インターネット環境について」をご確認ください。 ・「7.付録 C.インターネット接続確認方法」をご確認ください。
40%	証明書のエラーに関するメッセージが表示されている	「4.3.接続方法」をご確認ください。
48%	ID・パスワードが間違っている	ID・パスワードに誤りが無いかご確認ください。
	お客様にて制限されたアクセス元 IP アドレス以外から接続している	“Firewall ヒアリングシート”にて接続元 IP アドレスを制限していないかご確認ください。
80%	ID・パスワードが間違っている	ID・パスワードに誤りが無いかご確認ください。
	お客様にて制限されたアクセス元 IP アドレス以外から接続している	“Firewall ヒアリングシート”にて接続元 IP アドレスを制限していないかご確認ください。
	プロキシが原因で URL にアクセスできない	「7.付録 A.プロキシ設定手順」をご確認ください。
	Cookie が取得できていない	「2.2.4. 信頼済みサイトの設定」をご確認ください。
	ウイルス対策ソフト等で Cookie の取得を制限している	一度ウイルス対策ソフトを無効にした後、再接続してください。 もし、改善された場合はウイルス対策ソフトの設定を変更ください。
98%	ネットワークアダプタを変更する権限がない	「4.1.起動方法」をご確認ください。
	別のバージョンの FortiClient VPN がインストールされている	「6.異なるバージョンのアプリを使用する場合」をご確認ください。
	ネットワークアダプタが正常に動作していない	以下の手順でアプリを再インストールしてください。 1) コントロールパネルからプログラムのアンインストールを選択し、Forticlient SSLVPN をアンインストールします。
	WindowsUpdate 等でネットワークアダプタが破損した	2) PC を再起動します。 3) Forticlient SSLVPN を再インストールします。 4) PC を再起動します。

それでも SSL-VPN が繋がらない場合は、以下の情報を確認した上で、弊社までお問い合わせください。

- ①本事象は複数の PC で発生しているか。  
または、特定の PC のみで発生しているか。
- ②事象の発生している PC の OS とバージョン。  
(Windows10 1803、Windows11、など)
- ③ご利用のブラウザとバージョン。
- ④ご利用の FortiClient のバージョン。
- ⑤SSL-VPN ができないエラー状況。  
(可能であれば、スクリーンショットをご提供お願いします)

## C. インターネット接続確認方法

お客様 PC から弊社トンネル接続用 URL にアクセスできているか確認する方法について説明します。

- ① ご利用機能に応じて URL を Google Chrome 等のブラウザに入力し、アクセスします。

ご利用機能	[Server Address]に入力する URL
IaaS サービスにてインターネット経由で仮想マシンにアクセスする。	“SSL-VPN 設定情報”に記載されているログインページ URL を入力します。
オンラインストレージサービスにてインターネット経由でボリュームにアクセスする。	“SSL-VPN 設定情報”に記載されているログインページ URL を入力します。
IaaS3 サービスで WEB 操作画面・バックアップ・リストア操作画面にアクセスする。	“操作画面情報”に記載されているサイトアクセス情報の URL を入力します。

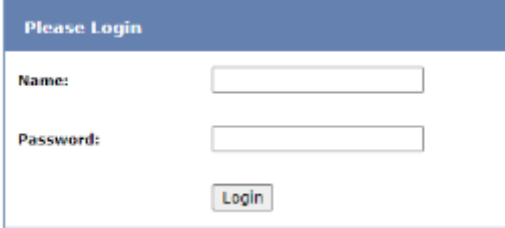
- ② 下記エラーが表示された場合、[詳細設定]をクリックし、[XXX.XXX.XXX.XXX にアクセスする（安全ではありません）] をクリックします  
※ブラウザにより表示内容が異なります。



図 7.C.1 インターネット接続確認方法 -1



- ③ 以下のログイン画面が表示されましたら弊社トンネル接続用 URL へのアクセスは問題ありません。



The image shows a login form with a blue header bar containing the text "Please Login". Below the header, there are two rows of labels and input fields. The first row is labeled "Name:" and has a white rectangular input box. The second row is labeled "Password:" and has a white rectangular input box. Below these two rows, there is a button labeled "Login".

図 7.C.2 インターネット接続確認方法 -2

ログイン画面が表示されない場合、以下の点についてご確認ください。

- ・ お客様ネットワーク管理者様に「2.2.1. インターネット環境について」をご確認ください。
  - ・ プロキシサーバーをご利用の場合、「7.付録 A.プロキシ設定手順」をご確認ください。
- ④ ログインする必要はありませんが、ご利用の ID・パスワードが正しいか確認する場合、  
"Name"、"Password"を入力し、[Login]をクリックします。  
ログインできましたら、ご利用の ID・パスワードは正しいです。  
なお、このページからトンネル接続はできませんのでそのままログアウトしてください。

## SSL-VPN 利用マニュアル

2011年11月15日	第1版
2022年11月15日	第6.24版
2023年10月2日	第7版
2024年2月5日	第8版
2024年3月29日	第9版

株式会社さくらケーシーエス  
データセンター

Copyright© 2011-2024 SAKURA KCS Corp. All Rights Reserved.

本書に記載されている情報、事項、データは、予告なく変更されることがあります。

本書を弊社に無断でその一部、あるいはその全部を複製、複製（コピー）、追加、削除、加工および転載することを禁じます。