SECURE CONNECT

Client Installation Manual

Manual Version:8.0

2023 年 1 月 6 日

OPTAGE

目 次

1．はじめに

1．1 SECURE CONNECT とは

株式会社オプテージが提供する、リモートアクセスサービスの名称です。
IoT-EX 社製の VPN ソフトウェア「L2Connect」を利用した SaaS 型 VPN 構築サービスで、リモートアクセスや拠点間接続を簡単、安全かつ安価に実現します。

SECURE CONNECT はソフトウェアにより作りだされる仮想スイッチを用いて、既存の IP ネットワーク上にオーバーレイネットワーク「**SECURE CONNECT** ネットワーク」を構築します。
お客様のパソコンから **SECURE CONNECT** ネットワークへの接続認証には、ID とパスワードを用いるのではなく、USB トークンに格納された電子証明書を用います。
この電子証明書による相互認証で接続を確立する仕組みを採用し、電子証明書がなければ **SECURE CONNECT** ネットワークとの接続はできません。そのため、高いセキュリティー機能を持つとともに簡単な操作で **SECURE CONNECT** ネットワーク接続を確立することができる仕組みとなっております。
本マニュアルでは、L2C クライアントのインストールと設定項目の説明、操作方法を解説します。

１．２　本マニュアルで使用する製品等の名称

1)　本マニュアルで表記した会社名、商品名は、各社の商標または登録商標です。

・ L2Connect は、IoT-EX 株式会社の商標です。

・ Windows は、米国 Microsoft Corporation の米国及びその他の国における商標または登録商標です。

・ 本文中及び図表中では、TM、®マークは表記しておりません。

2)　**SECURE CONNECT** で使用する L2Connect 製品

・ L2C クライアント　(製品名称：L2Connect Remote Access for Windows)

お客様のパソコンにインストールする VPN ソフトです。

L2C クライアントは L2C サーバに接続し、VPN 経路を構築いたします。

・ L2C ブリッジ　(製品名称：L2Connect Embedded)

お客様拠点に設置する VPN 装置です。L2C ブリッジは L2C サーバに接続し、VPN 経路を構築するとともに、お客様拠点にある機器の通信を L2C サーバに転送いたします。

・ L2C サーバ　(製品名称：L2Connect Server)

接続されている L2C クライアントや L2C ブリッジ間で、通信を中継いたします。これによりリモートアクセスや拠点間接続が可能となります。

3)　USB トークン

SECURE CONNECT で使用する、認証用の USB 機器です。

L2C クライアントによる VPN 接続時に、本 USB トークンをお客様のパソコンに接続し認証をすることで、よりセキュアな VPN を確立することができます。

・ ePass2003

Windows10 及び Windows11 に対応している USB トークンの製品名称です。

4) 電子証明書

USB トークンに内蔵されており、L2C クライアントが L2C サーバと VPN 接続をするための身分証明書の役割を果たします。
L2C クライアントと L2C サーバは、公開鍵基盤(PKI)に基づいたユーザ認証及びサーバ認証を行うため、本電子証明書が必要となります。

5) L2Connect 仮想ネットワークデバイス

L2C クライアントをインストールすると、自動的にインストールされる仮想的なネットワークデバイスです。
L2Connect 仮想ネットワークデバイスは、1 枚の物理的なネットワークデバイスと同等に認識され、インターネットプロトコル(TCP/IP) を物理的なネットワークデバイスと同様に設定することができます。

6) PIN (SO PIN、ユーザ PIN)

USB トークン内の接続データにアクセスするためのパスワードです。

・ SO PIN

USB トークンの管理を行うためのパスワードです。
ユーザ PIN の変更や PIN ブロックした USB トークンを再度使用できるようにする際に使用します。

※SO PIN の入力を 10 回連続で間違えると、USB トークン自体が使えなくなりますのでご注意下さい。

・ ユーザ PIN

SECURE CONNECT を利用されるユーザ向けのパスワードです。
USB トークンをパソコンに接続後、L2C サーバと VPN 接続する際に入力を求められます。

※ユーザ PIN の入力を 10 回連続で間違えると、PIN ブロックされ USB トークンが一時的に使えなくなりますのでご注意下さい。PIN ブロックの解除が必要となります。

7) 管理ツール(ePass マネージャ)

SO PIN、ユーザ PIN の変更や、PIN ブロックした USB トークンを再度使用できるようにする際に使用します。

1．3 SECURE CONNECT の動作環境

SECURE CONNECT は、表 1-1 の環境で動作します。

表 1-1 **SECURE CONNECT** 動作環境

動作確認OS*1	Windows 10 (32bit 版、64bit 版) Windows 11 (64bit 版) Windows Server 2012 R2 (64bit 版) Windows Server 2016 (64bit 版) Windows Server 2019 (64bit 版)
CPU*2	Intel PentiumⅢ800MHz相当またはそれ以上のCPU
メモリ*2	512Mbytes
ハードディスク*2	Cドライブに最低15Mbytes以上の空き容量 (1.5Gbytes以上推奨)
ネットワーク環境	TCP/IP (IPv4) をサポートするネットワーク (Ethernet接続またはPPPなどダイヤルアップ接続に対応)

*1:各 OS の正式名称ではなく、略称で記載しています。

*2:各 OS の最小システム要件が満たされていることを前提としています。

１．４　SECURE CONNECT サービスを利用するための準備物

本マニュアルに沿った手順を行う場合、下記準備物を事前にご用意下さい。

1) お客様のパソコン
2) USB トークン
3) USB トークンドライバ及び L2C クライアントのインストーラ※

※サービスご利用開始時にお渡しした、インストールメディアをご用意ください。
※インストールメディアがお手元にない場合、**SECURE CONNECT** サポート窓口に
お問い合わせください。**SECURE CONNECT** サポート窓口につきましては、
「8.1 **SECURE CONNECT** サポートサイト」をご参照ください。

4) L2Connect 仮想ネットワークドライバの設定情報
お客様のネットワーク環境の IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバのアドレスが必要です。

※お客様のネットワーク環境に DHCP サーバがある場合は、自動的に取得することも可能です。

5) Proxy サーバの設定情報
お客様のネットワーク環境における、Proxy サーバの情報が必要です。

※ユーザ認証が必要な HTTP プロキシサーバの一部には、NTLM 認証にのみ対応しているものがあります。L2C クライアントは NTLM 認証に対応していないため、NTLM 認証を要求する HTTP プロキシサーバを経由して通信することはできません。

１．５　その他

１）本マニュアルは、Windows10 における Pass2003 を基に作成しております。
他の OS 及び USB トークンでインストールする際は、名称や表示画面が異なる場合がございますので、ご了承下さい。

２）USB トークンの種別の見分け方につきましては、USB トークンに貼付しているシール表 1-2 にて、ご確認下さい。

表 1-2　USB トークンの種別の見分け方

USB トークンの種別	貼付シール
ePass2003	「ePass2003」、「デバイス ID」が記載されたシール

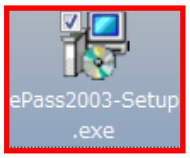
2. SECURE CONNECT のインストールと設定

2．1　USB トークンドライバ(ePass2003)のインストール

※管理者権限のあるユーザで実施して下さい。
※USB トークンドライバは複数の種類で共存することが可能となっております。
以前に利用されていた USB トークンドライバをアンインストールする必要はございません。

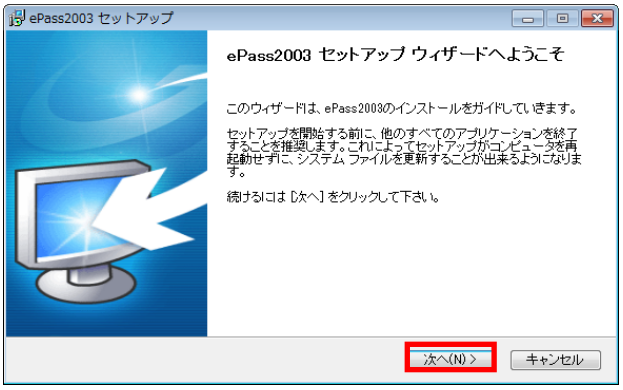
1）付属されている CD-ROM の「インストール CD 」-「PC」-「install」-「ePass2003」フォルダ内にある　「ePass2003-Setup.exe」アプリケーションをダブルクリックして下さい。

※サービスご利用開始時にお渡しした、インストールメディアをご用意ください。
※インストールメディアがお手元にない場合、SECURE CONNECT サポート窓口にお問い合わせください。SECURE CONNECT サポート窓口につきましては、「8.1 SECURE CONNECT サポートサイト」をご参照ください。

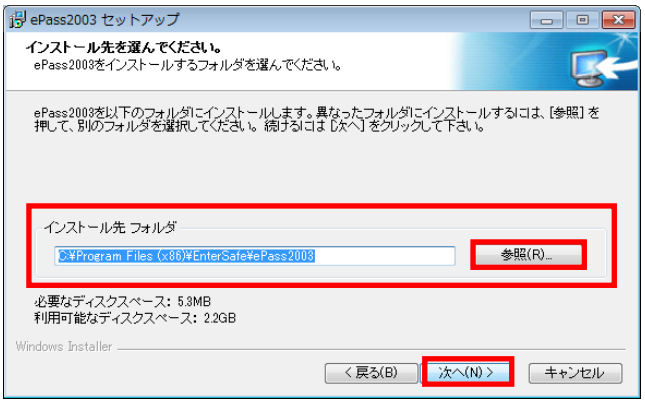


※セキュリティの警告またはユーザアカウント制御が表示された場合は、「はい」をクリックして下さい。
※インストール中、USB トークンは接続しないで下さい。

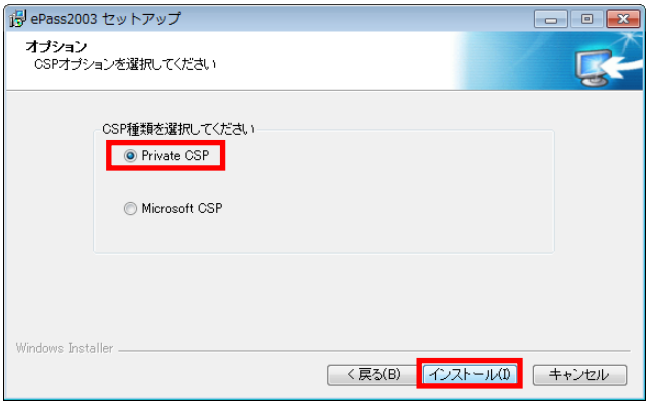
2）セットアップ画面が表示されますので、「次へ」をクリックして下さい。



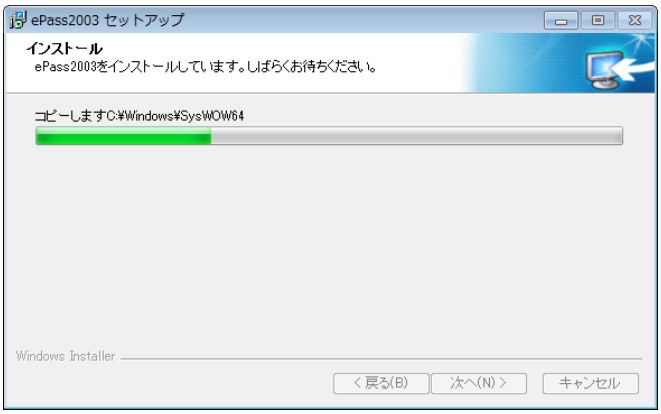
3）「インストール先を選んでください。」と表示されますので、特に変更する必要がない場合は、そのまま「次へ」をクリックして下さい。
変更する場合は、「インストール先フォルダ」の「参照」をクリックし、インストール先フォルダを選択後、「次へ」をクリックして下さい。



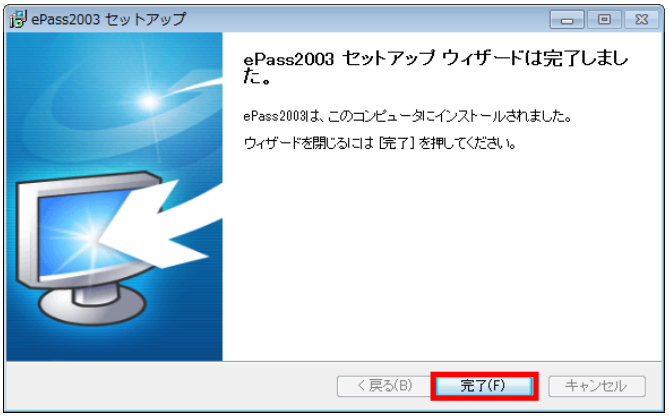
4）オプション画面が表示されますので、「Private CSP」を選択し、「インストール」をクリックして下さい。



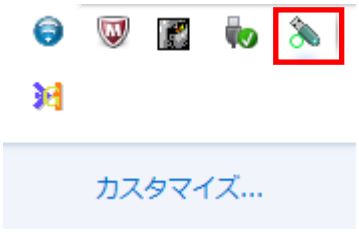
５）ePass2003 のインストール実行中の画面が表示されます。



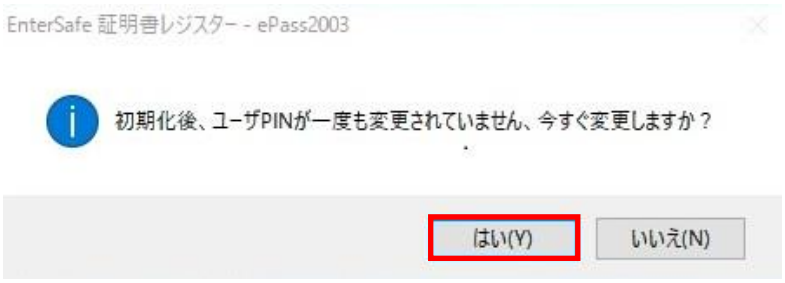
６）インストールが実行されますので、下記画面の「完了」をクリックして下さい。



7）USB トークンを接続すると自動でセットアップ処理が開始され、セットアップ完了後、タスクトレイに下記画面のようなアイコンが表示されます。



8）出荷された状態の USB トークンを初めてパソコンに接続した際、「ユーザ PIN の変更」画面が表示される場合があります。その際は「OK」をクリックし、ユーザ PIN を変更して下さい。



※ユーザ PIN を変更するまで、上記画面は表示されます。

以上で、USB トークンドライバ（ePass2003）のインストールは完了です。

接続を実施する際には、ユーザ PIN の入力が必要となります。
初期のユーザ PIN は以下のルールで登録されています。

（初期ユーザ PIN ルール）デバイス ID 下 2 桁 ＋ ユーザ ID 下 6 桁

※申請時のユーザ ID が 6 桁に満たない場合は、6 桁になるよう
ユーザ ID の後に「0」を追加して設定しています。

＜初期ユーザ PIN 例＞ デバイス ID が「1234567890ab」、ユーザ ID が ABCDEFGH の場合
（初期ユーザ PIN） abCDEFGH

注意

ご使用になられる前に、必ず初期ユーザ PIN から自分だけが分かるユーザ PIN に変更して下さい。設定方法につきましては、「４．３ ユーザ PIN の変更(ePass2003)」をご参照下さい。

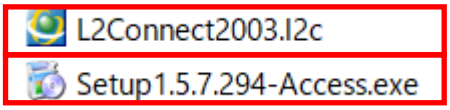
２．２　L2C クライアントのインストール

※管理者権限のあるユーザで実施して下さい。

１）付属されている CD-ROM の「インストール CD 」-「PC」-「install」-「L2Connect Remote Access for Windows」フォルダを選択して下さい。

※サービスご利用開始時にお渡しした、インストールメディアをご用意ください。
※インストールメディアがお手元にない場合、SECURE CONNECT サポート窓口に
お問い合わせください。SECURE CONNECT サポート窓口につきましては、
「8.1 SECURE CONNECT サポートサイト」をご参照ください。

２）接続プロファイル（拡張子 l2c）と L2C クライアントインストーラ（拡張子 exe）が同じフォルダにあることを確認し、L2C クライアントインストーラを実行して下さい。



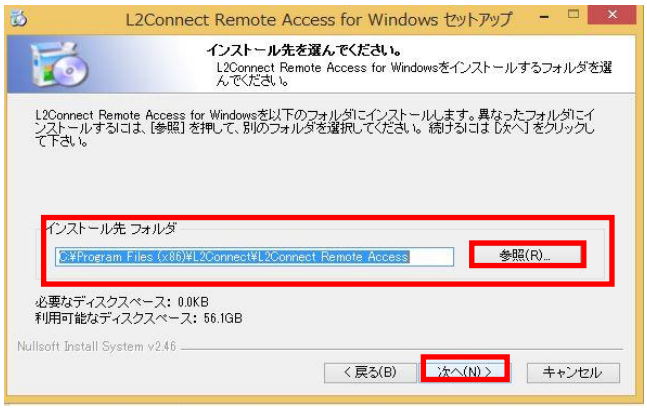
※L2C クライアントのバージョンにつきましては、表記と異なる場合がございます。
※接続プロファイルは、L2C クライアントインストーラと同じフォルダ内にある状態で
インストールを実行することで、自動的にインポートされます。
※セキュリティの警告またはユーザアカウント制御が表示された場合は、「はい」をクリック
して下さい。

USB トークンの種別	接続プロファイルの種別
ePass2003	L2Connect2003.l2c

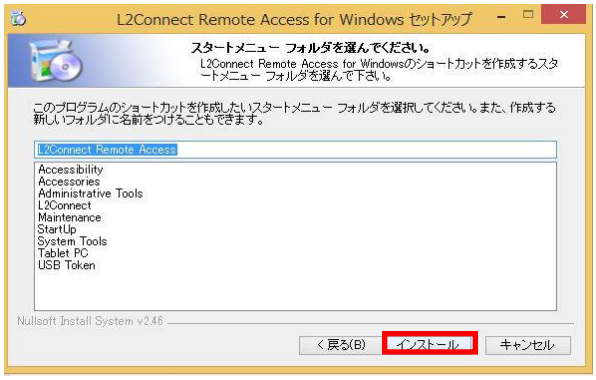
３）セットアップ画面が表示されますので、「次へ」をクリックして下さい。

４）「L2Connect 使用許諾契約書」が表示されますので、「このライセンス契約書に同意します。」にチェックを入れ、「次へ」をクリックして下さい。

５）「インストール先を選んでください。」と表示されますので、特に変更する必要がない場合は、そのまま「次へ」をクリックして下さい。
変更する場合は、「インストール先フォルダ」の「参照」をクリックし、インストール先フォルダを選択後、「次へ」をクリックして下さい。



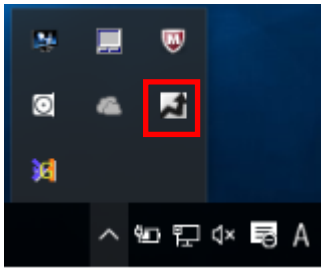
６）「インストール」をクリックして、インストールを開始して下さい。



７）インストールの実行画面が表示されます。

８）インストールが完了すると完了画面が表示されますので、「完了」をクリックして下さい。

９）インストールが完了し再起動されると、タスクトレイに L2C クライアントのアイコンが表示されます。



以上で、L2C クライアントのインストールは完了です。

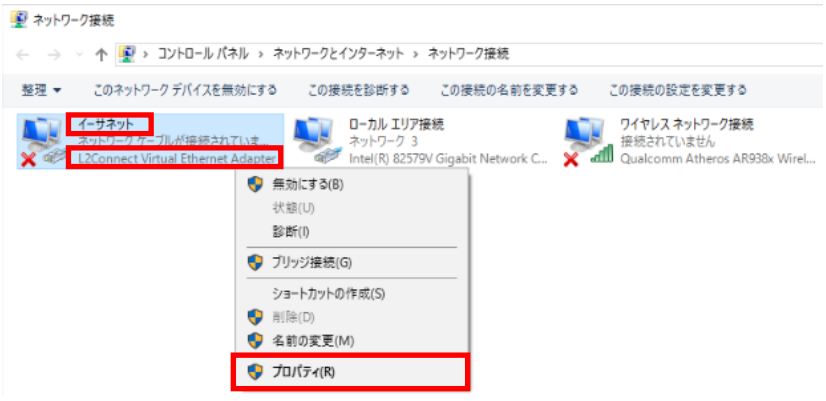
２．３　L2Connect 仮想ネットワークデバイスの設定

※管理者権限のあるユーザで実施して下さい。

※設定内容は、ネットワーク管理者の指示に従って変更して下さい。

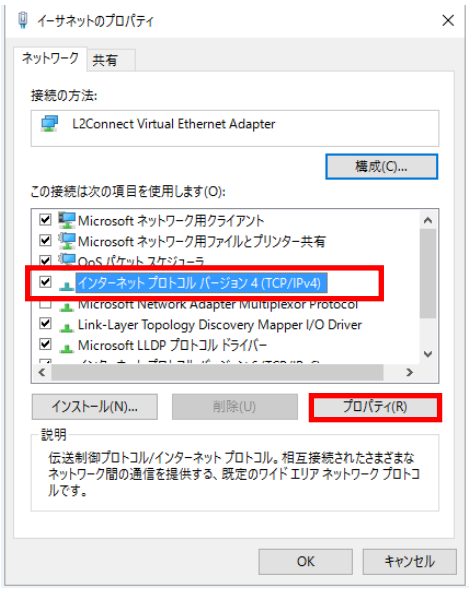
１）「デスクトップ」 －「コントロールパネル」－「ネットワークと共有センター」－「アダプターの設定の変更」を開いて下さい。

２）「イーサネット　L2Connect Virtual Ethernet Adapter」アイコンを右クリックし、「プロパティ」をクリックして下さい。



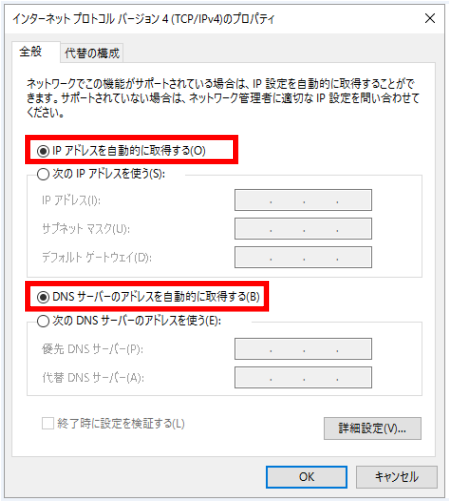
※上記画面のネットワークデバイス名が「イーサネット」と表記されておりますが、
お客様の環境によりネットワークデバイス名の表記が異なる場合がございます。
必ず「L2Connect Virtual Ethernet Adapter」と記載されているものを設定して下さい。

３）仮想 LAN カードのネットワーク設定を変更することができる画面が表示されますので、「インターネット プロトコル バージョン 4(TCP/IPv4)」を選択し、「プロパティ」をクリックして下さい。



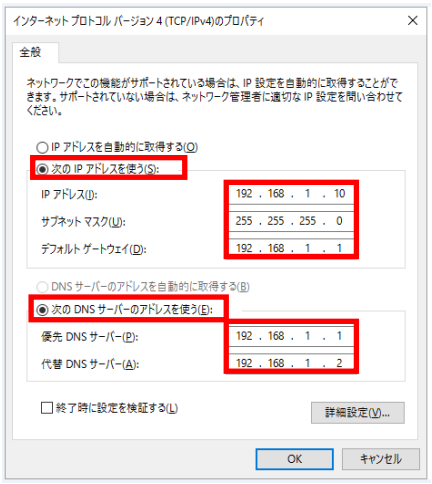
４）IP アドレス及び DNS サーバアドレスを設定して「OK」をクリックして下さい。

A) IP アドレス及び DNS サーバアドレスが、仮想ネットワーク内の DHCP サーバによって自動的に割り当てられる場合、「IP アドレスを自動的に取得する」及び「DNS サーバーのアドレスを自動的に取得する」を選択して下さい。



※L2C クライアントをインストールした時点では、「IP アドレスを自動的に取得する」及び「DNS サーバーのアドレスを自動的に取得する」が選択されています。

B) IP アドレス及び DNS サーバアドレスをユーザが固定的に割り当てる場合は、
「次の IP アドレスを使う」をクリックして下さい。
「IP アドレス」、「サブネット マスク」、「デフォルトゲートウェイ」の項目が、入力可能になります。
ネットワーク管理者から指定された「IP アドレス」、「サブネット マスク」、「ゲートウェイ」のアドレスを入力して下さい。
同様に DNS サーバアドレスを指定する必要がある場合は、DNS サーバの IP アドレスを入力して下さい。



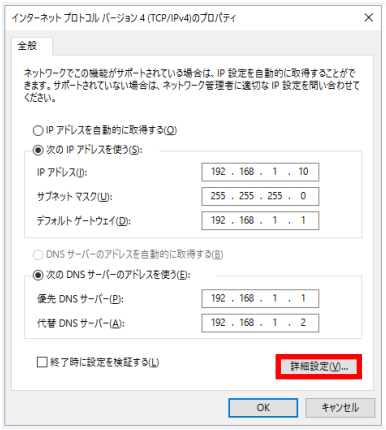
※上記画面のネットワーク設定は一例です。

C) 「TCP/IP」の詳細設定

利用するネットワークの構成によっては、より詳しい「TCP/IP」の設定が必要な場合があります。

「TCP/IP」の詳細設定を行うためには、「インターネットプロトコルバージョン4(TCP/IPv4)」のプロパティ画面において、「詳細設定」をクリックして下さい。

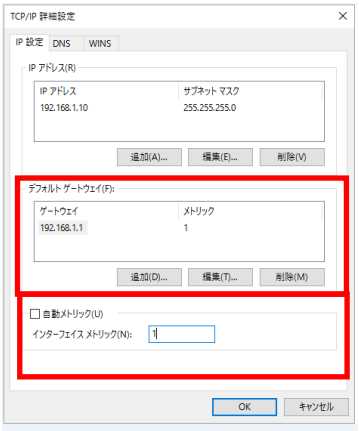
「詳細設定」画面では、「IP 設定」、「DNS」、「WINS」、「オプション」などの詳細な設定を行うことができます。



※上記画面のネットワーク設定は一例です。

L2Connect 仮想ネットワークデバイス経由でインターネットへ接続する場合は、下記の通り設定します。

- デフォルトゲートウェイメトリックの値を「１」に設定
- インターフェイスメトリックの値を「１」に設定



※上記画面の IP アドレス設定は一例です。

※一度設定された内容は、変更しない限り継続して使用されます。

以上で、L2Connect 仮想ネットワークデバイスの設定は完了です。

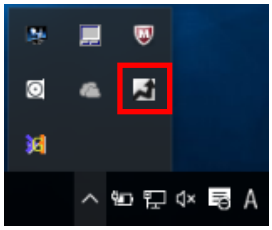
２．４　Proxy の設定

※管理者権限のあるユーザで実施して下さい。

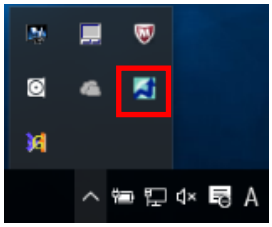
※お客様ネットワーク環境に Proxy サーバがある場合、Proxy の設定が必要となります。
Proxy を使用せず直接インターネット接続を行っている場合、設定は不要です。

※ユーザ認証が必要な HTTP プロキシサーバの一部には、NTLM 認証にのみ対応しているものがあります。L2C クライアントは 、NTLM 認証に対応していないため NTLM 認証を要求する HTTP プロキシサーバを経由して通信することはできません。

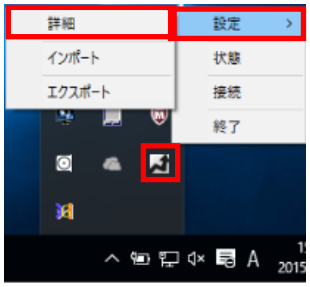
１）L2Connect の矢印アイコンの色が灰色であることを確認して下さい。



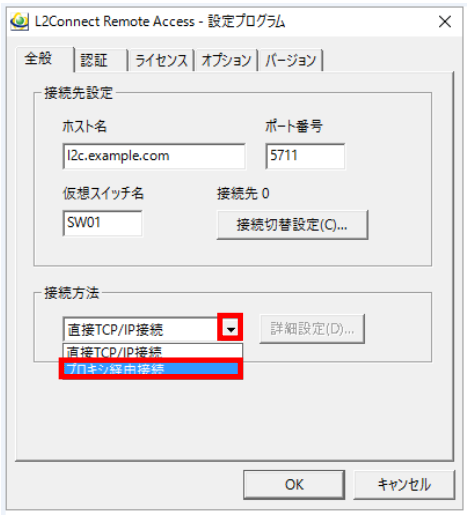
※L2Connect の矢印アイコンの色が青色の場合は、「３．３　L2C サーバとの接続の切断」を参照し、接続を終了して下さい。



２）L2Connect の矢印アイコンを右クリックし、ポップアップメニューから「設定」-「詳細」をクリックして下さい。



3）接続方法のプルダウンをクリックし、「プロキシ経由接続」を選択して下さい。

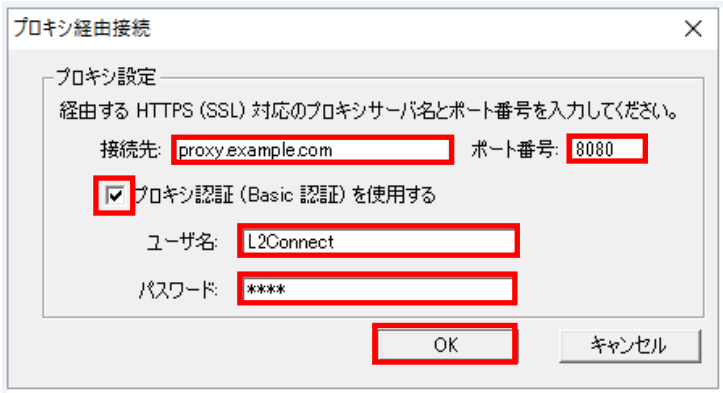


※上記画面の設定値は一例です。

4）「詳細設定」ボタンをクリックして下さい。

※上記画面の設定値は一例です。

５）接続先プロキシサーバ名、または IP アドレスと接続ポート番号を入力し、「OK」をクリックして下さい。
プロキシ認証（Basic 認証）を使用する場合は、プロキシ認証(Basic 認証)のチェックボックスにチェックを入れ、ユーザ名とパスワードを入力し、「OK」をクリックして下さい。



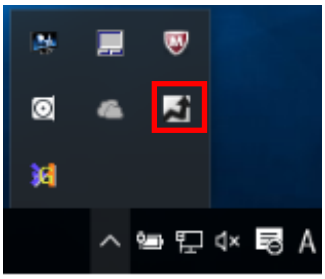
※上記画面の設定値は一例です。

以上で、Proxy の設定は完了です。

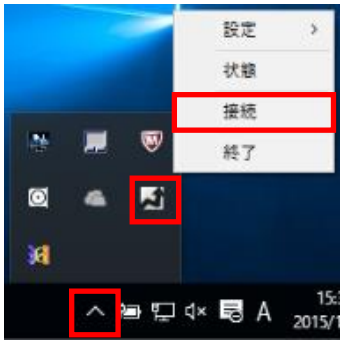
3．SECURE CONNECT の操作

3．1　L2C サーバへの接続

1）L2C クライアントを起動して下さい。起動後、右下タスクバーに L2Connect の矢印アイコンが表示されますので、USB トークンを接続して下さい。

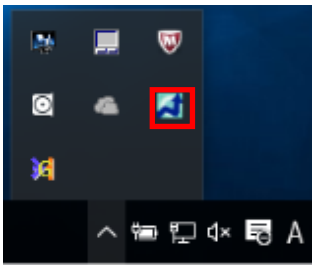


2）L2Connect の矢印アイコンを右クリックし、「タスクトレイメニュー」－「接続」を選択し、「ログイン」画面を表示して下さい。
または L2Connect の矢印アイコンをダブルクリックし、「ログイン」画面を表示して下さい。



３）ログイン画面が表示されるので、「ユーザ PIN」を入力し、「接続」ボタンをクリックして下さい。
L2C サーバへの接続を開始します。

４）L2C サーバへの接続が完了すると、L2Connect の矢印アイコンが「接続完了」状態（青色）になります。



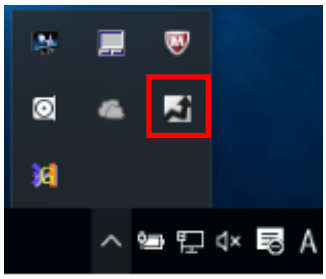
※L2C サーバへの接続に失敗した場合、L2C クライアントは接続が完了するまで、接続処理を繰り返します。ただし、500 回（約 8 時間）連続で失敗すると接続処理を終了します。

以上で、L2C サーバへの接続は完了です。

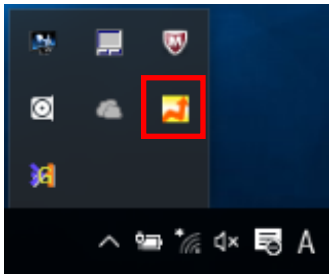
３．２　接続状態の表示

L2C クライアントの L2C サーバへの接続状態は L2Connect の矢印アイコンの色で確認することができます。
L2Connect の矢印アイコンは、L2C サーバとの接続状態に応じて下記画面のように変化します。

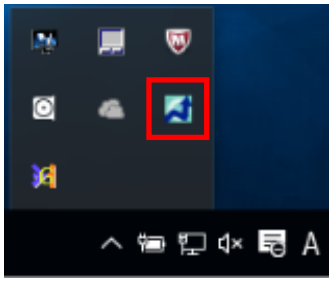
- 灰色…L2C サーバと未接続の状態



- 黄色…L2C サーバと接続中の状態

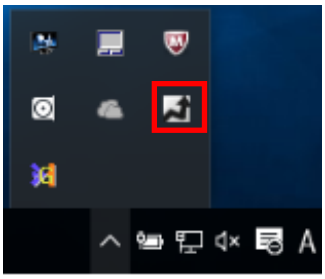


- 青色…L2C サーバと接続完了の状態

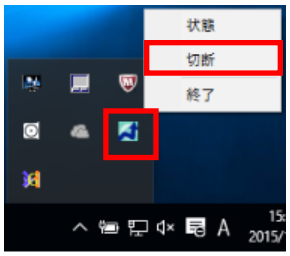


３．３　L2C サーバとの接続の切断

１）L2C クライアント設定プログラムが起動していない場合、L2C クライアントを起動して下さい。起動後、右下タスクバーに L2Connect の矢印アイコンが表示されます。



２）L2Connect の矢印アイコンアイコンを右クリックし、「タスクトレイメニュー」－「切断」をクリックして下さい。



※「切断」をせずに「終了」や「シャットダウン」、「再起動」、USB トークンを抜くなどを行った場合、L2C サーバとの切断処置が正常に行われず、次回以降接続時に以下のエラー画面が表示される可能性がございます。必ず「切断」を実施いただきますようお願いいたします。

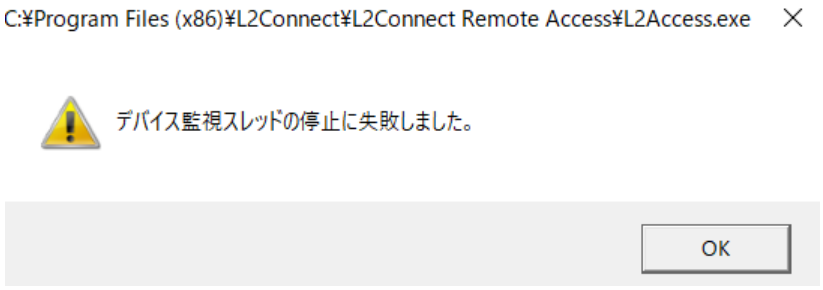
以上で、L2C サーバとの接続の切断は完了です。

３．４　Windows オペレーティングシステムからログオフした場合の挙動

L2C クライアントが L2C サーバに接続されている状態で、Windows オペレーティングシステムからログオフした場合、L2C サーバとの接続は切断されますが、正常な手順で終了していない為、エラー画面が表示されたり、セッションが残留し次回接続時に接続不可になる場合があります。

Windows オペレーティングシステムを「シャットダウン」、「再起動」した場合、L2C クライアント設定プログラムにより L2C サーバとの接続は切断されます。こちらも、ログオフ時と同様に、正常な手順で終了していない為、エラー画面の表示やセッションが残留し次回接続時に接続不可になる場合があります。
また長時間 L2C サーバと接続ができない場合、自動的に「切断」状態となります。

※「切断」をせずに「終了」や「シャットダウン」、「再起動」、USB トークンを抜くなどを行った場合、L2C サーバとの切断処置が正常に行われず、次回以降接続時に以下のエラー画面が表示される可能性がございます。必ず「切断」を実施いただきますようお願いいたします。



４．USB トークンの管理ツール(ePass マネージャ)

４．１　管理ツール(ePass マネージャ)

ユーザ PIN の変更、PIN ブロックされた USB トークンの解除の際には、CD-ROM に同梱されている管理ツール(ePass マネージャ)を使用します。

※サービスご利用開始時にお渡しした、インストールメディアをご用意ください。
※インストールメディアがお手元にない場合、SECURE CONNECT サポート窓口に
お問い合わせください。SECURE CONNECT サポート窓口につきましては、
「8.1 SECURE CONNECT サポートサイト」をご参照ください。

USB トークンの種別	USB トークンマネージャインストールファイル名
ePass2003	ePassManagerAdm_2003.exe

管理ツール(ePass マネージャ)を使用するには、管理ツール(ePass マネージャ)を起動するパソコンに USB トークンドライバがインストールされている必要があります。
USB トークンドライバのインストールにつきましては、「２．１　USB トークンドライバ(ePass2003)のインストール」をご参照下さい。

４．２　USB トークンの PIN ブロック

USB トークンの PIN ブロック
ユーザ PIN の入力を１０回連続で間違えると、USB トークンが PIN ブロックされ使用できなくなります。

※USB トークンが PIN ブロックされた場合には、L2Connect Remote Access（L2C クライアント）のポップアップメッセージ、ログに「PIN コードがロックされています」と表示されます。
USB トークンが PIN ブロックされた場合、管理ツール(ePass マネージャ)を使用し PIN ブロックを解除して下さい。

※PIN ブロックの解除には、SO PIN（管理者 PIN）が必要となります。

※SO PIN につきましては、お客様の **SECURE CONNECT** 管理者の方のみに通知しております。

※弊社ヘルプデスク窓口ではセキュリティ上、SO PIN をお教えすることはできません。

※SO PIN がご不明な方につきましては、お客様の **SECURE CONNECT** 管理者の方にお問い合わせ下さい。

※SO PIN がご不明な **SECURE CONNECT** 管理者の方につきましては、弊社担当営業にまでお問い合わせ下さい。

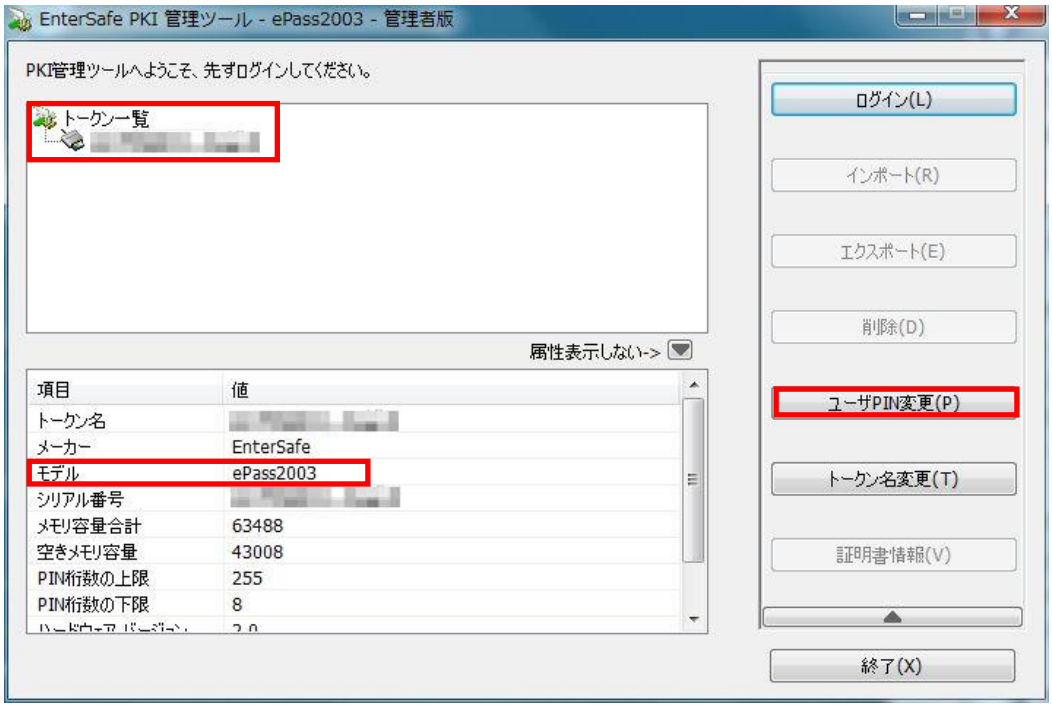
４．３　ユーザ PIN の変更(ePass2003)

１）ユーザ PIN を変更する USB トークンを接続し、ePass2003 管理ツールのアイコンまたは右下タスクバーに表示される下記トークンのアイコンをダブルクリックして、管理ツールを起動して下さい。

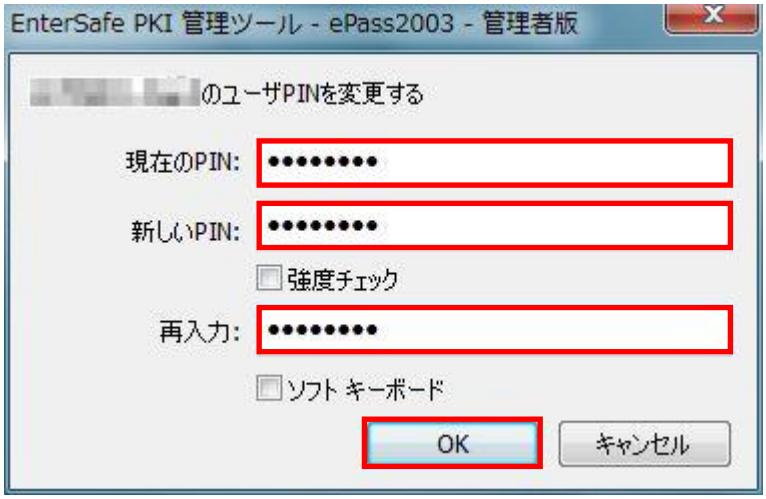
または

※セキュリティの警告またはユーザアカウント制御が表示された場合は、「はい」をクリックして下さい。

２）管理ツール(ePass マネージャ)の画面が表示されますので、スロットリストに認識されたデバイスを選択し、「ユーザ PIN 変更」ボタンをクリックして下さい。

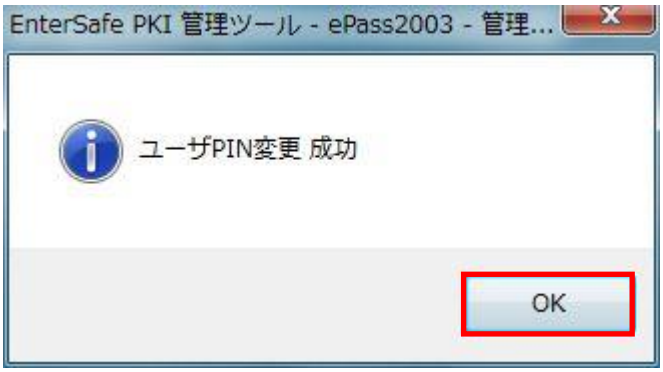


３）「現在のユーザ PIN」、「新しいユーザ PIN」及び「再入力（新しいユーザ PIN と同じもの）」を入力し、「OK」をクリックして下さい。（入力内容は非表示となります。）



※新しいユーザ PIN は、半角英数字で、4 文字以上 120 文字以下で入力して下さい。

４）ユーザ PIN が変更されますので、「OK」をクリックして下さい。



以上で、ユーザ PIN の変更は完了です。

４．４　ユーザ PIN ブロックの解除(ePass2003)

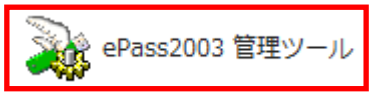
※PIN ブロックの解除には SO PIN が必要です。

※SO PIN につきましては、お客様の **SECURE CONNECT** 管理者の方のみに通知しております。

※弊社ヘルプデスク窓口ではセキュリティ上、SO PIN をお教えすることはできません。

※SO PIN がご不明な **SECURE CONNECT** 管理者の方につきましては、弊社担当営業にまでお問い合わせ下さい。

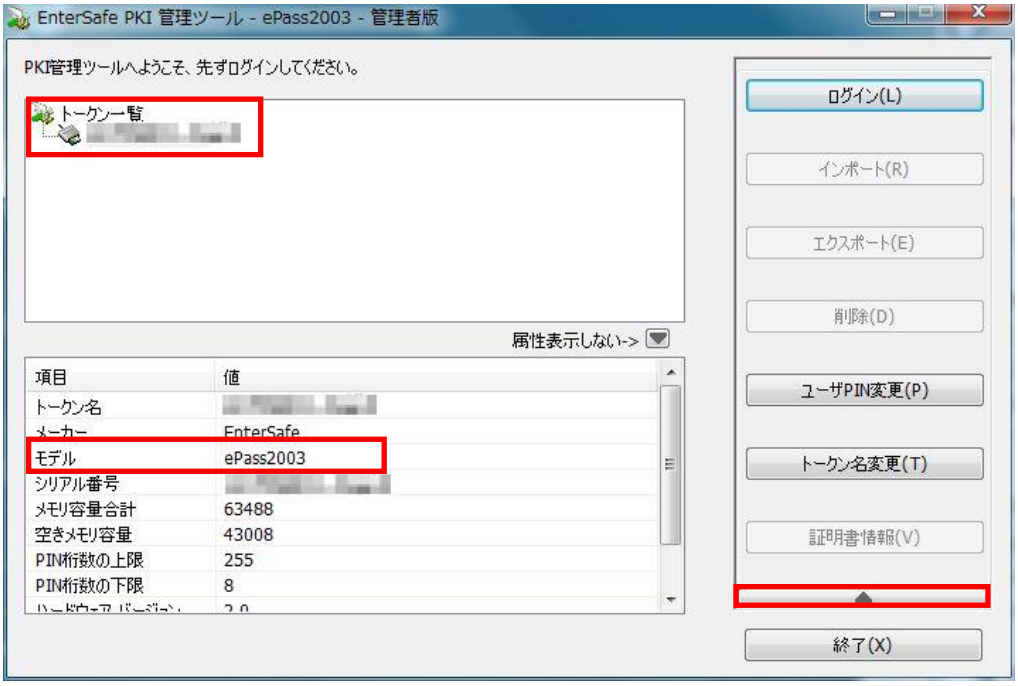
１）PIN ブロックを解除したい USB トークンを接続し、ePass2003 管理ツールのアイコンまたは右下タスクバーに表示される下記アイコンをダブルクリックし、管理ツールを起動します。



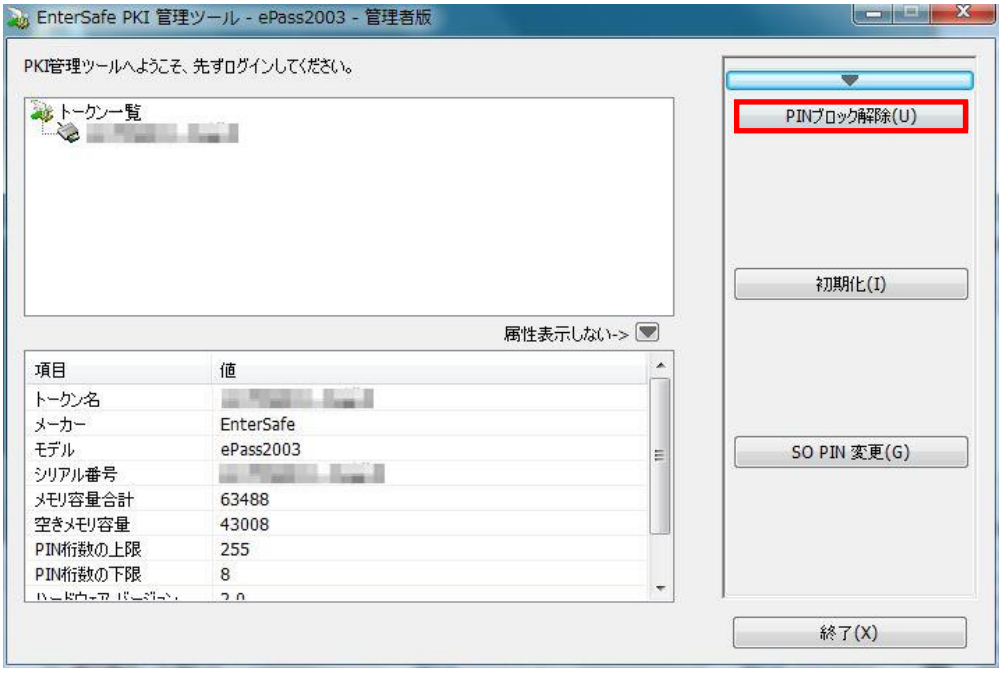
または

※セキュリティの警告またはユーザアカウント制御が表示された場合は、「はい」をクリックして下さい。

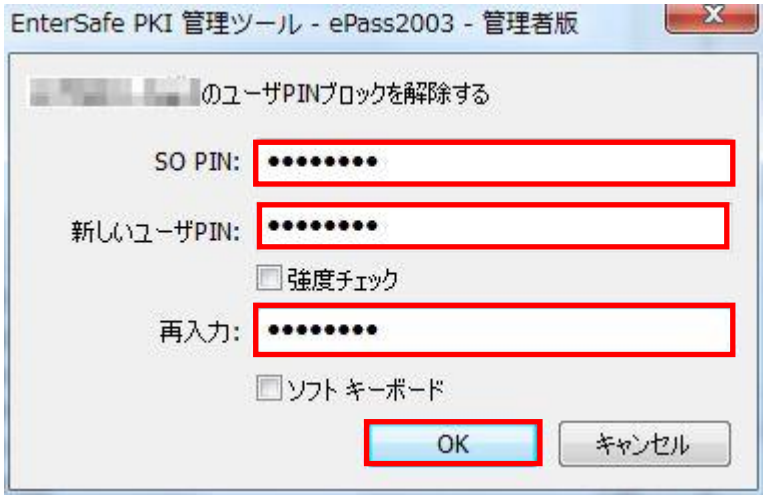
２）管理ツール（ePass マネージャ）の画面が表示されますので、スロットリストに認識されたデバイスを選択し、右メニュー下段にある「▲」クリックし、次画面へ移動して下さい。



３）「PIN ブロック解除」ボタンをクリックして下さい。



４）「SO PIN」、「新しいユーザ PIN」及び「再入力（新しいユーザ PIN と同じもの）」を入力します。（入力内容は非表示となります。）



※新しいユーザ PIN は、半角英数字で、4 文字以上 120 文字以下で入力して下さい。

５）PIN ブロックが解除されますので、「OK」をクリックします。
その後、USB トークンは再使用可能になります。

以上で、PIN ブロックの解除は完了です。

４．５　ユーザ PIN のリセット(ePass2003)

ユーザ PIN を忘れてしまった場合は ePass マネージャを使用し、ユーザ PIN を任意のものに変更することができます。
「４．４　ユーザ PIN ブロックの解除(ePass2003)」と同じ手順でユーザ PIN のリセットを実施して下さい。

※ユーザ PIN をリセットするには SO PIN が必要です。

※SO PIN につきましては、お客様の **SECURE CONNECT** 管理者の方のみに通知しております。

※弊社ヘルプデスク窓口ではセキュリティ上、SO PIN をお教えすることはできません。

※SO PIN がご不明な **SECURE CONNECT** 管理者の方につきましては、弊社担当営業にまでお問い合わせ下さい。

5．SECURE CONNECT のアップグレード

5．1　L2C クライアントのアップグレード

※管理者権限のあるユーザで実施して下さい。

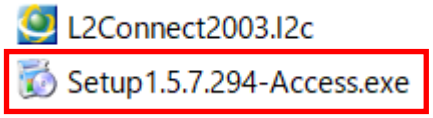
※アップグレード（上書きインストール）時、既存の設定情報が引き継がれます。

1）付属されている CD-ROM の「インストール CD 」-「PC」-「install」-「L2Connect Remote Access for Windows」フォルダを選択して下さい。

※サービスご利用開始時にお渡しした、インストールメディアをご用意ください。

※インストールメディアがお手元にない場合、**SECURE CONNECT** サポート窓口にお問い合わせください。**SECURE CONNECT** サポート窓口につきましては、「8.1 **SECURE CONNECT** サポートサイト」をご参照ください。

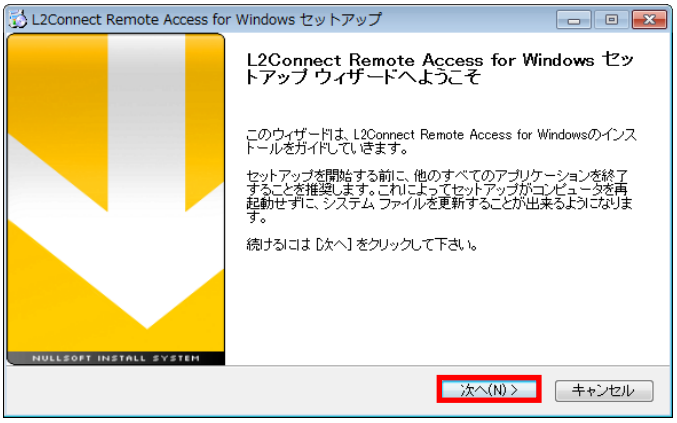
2）L2C クライアントインストーラ（拡張子 exe）を実行して下さい。



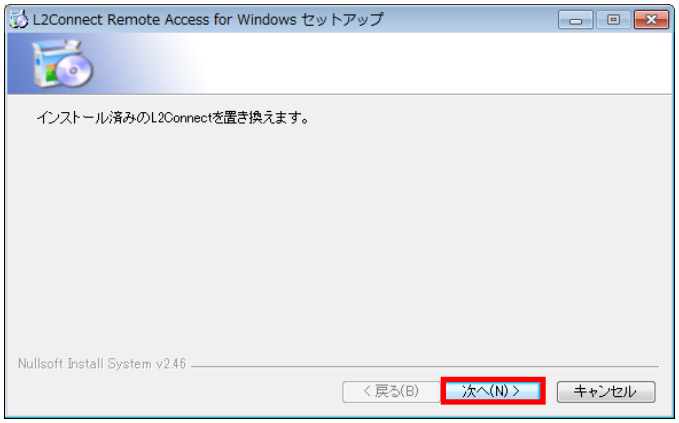
※L2C クライアントのバージョンにつきましては、表記と異なる場合がございます。

※セキュリティの警告またはユーザアカウント制御が表示された場合は、「はい」をクリックして下さい。

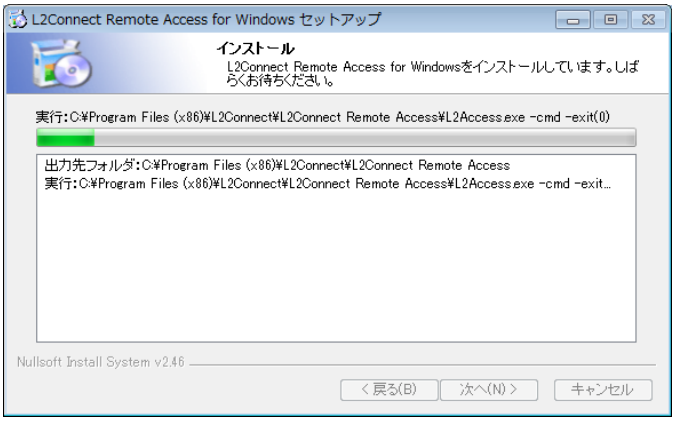
3）セットアップ画面が表示されますので、「次へ」をクリックして下さい。



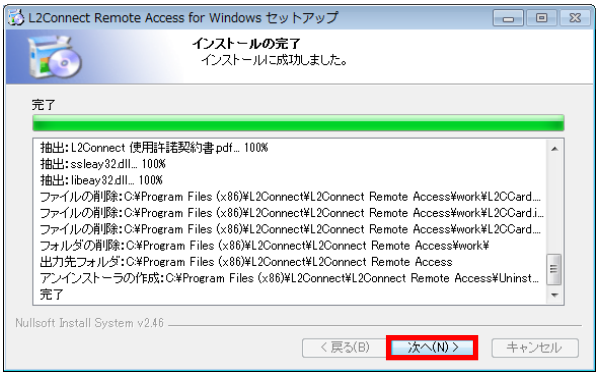
4）「インストール済の L2Connect を置き換えます。」のメッセージ画面が表示されますので、「次へ」をクリックして下さい。



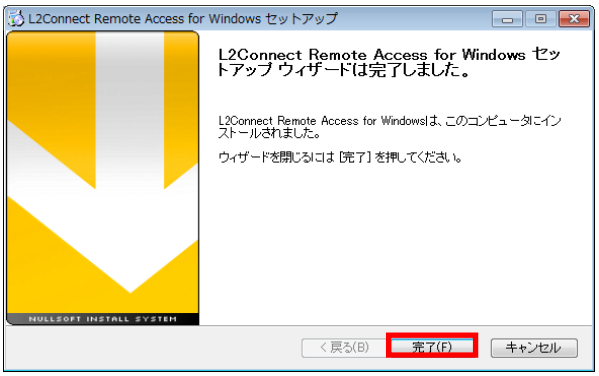
5）インストールの実行画面が表示されます。



6）インストールが完了すると完了画面が表示されますので、「次へ」をクリックして下さい。



7）セットアップウィザード完了画面が表示されますので、「完了」をクリックして下さい。



以上で、L2C クライアントのアップグレードは完了です。

６．SECURE CONNECT のアンインストール

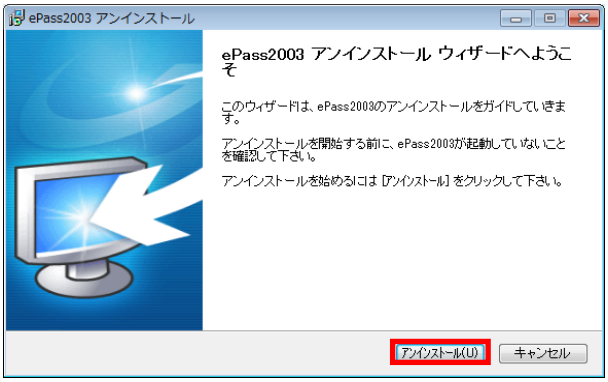
６．１　USB トークンドライバ(ePass2003)のアンインストール

※管理者権限のあるユーザで実施して下さい。

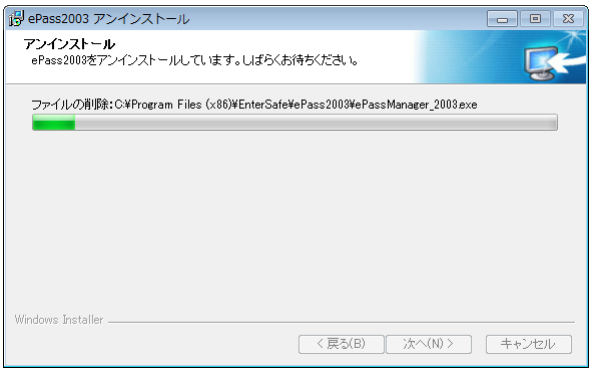
１)「３．３　L2C サーバとの接続の切断」を参照し、L2C サーバとの接続を切断して下さい。

２)「デスクトップ」－「コントロールパネル」－「プログラムと機能」を起動後、「ePass2003」を選択し、「アンインストール」をクリックしてアンインストールを実行して下さい。

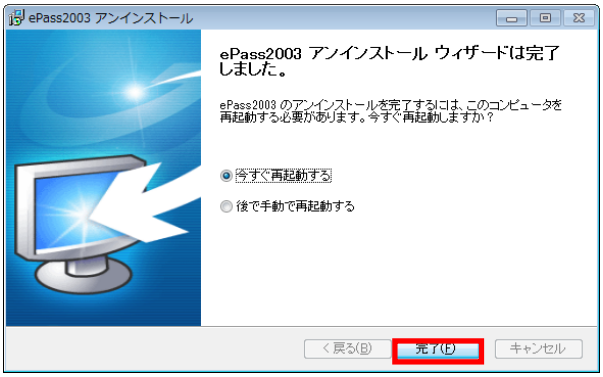
３) USB トークンドライバ(ePass2003)の削除を確認されますので、「アンインストール」をクリックして下さい。



４）USB トークンドライバ(ePass2003)のアンインストール実行中の画面が表示されます。



５）USB トークンドライバ(ePass2003)がアンインストールされた後、再起動を求めるダイアログが表示されますので、「完了」をクリックして下さい。
パソコンが再起動されます。
（再起動されない場合は、実行しているプログラムを全て終了し、シャットダウンメニューから再起動をクリックして下さい。）



以上で、USB トークンドライバ(ePass2003)のアンインストールは完了です。

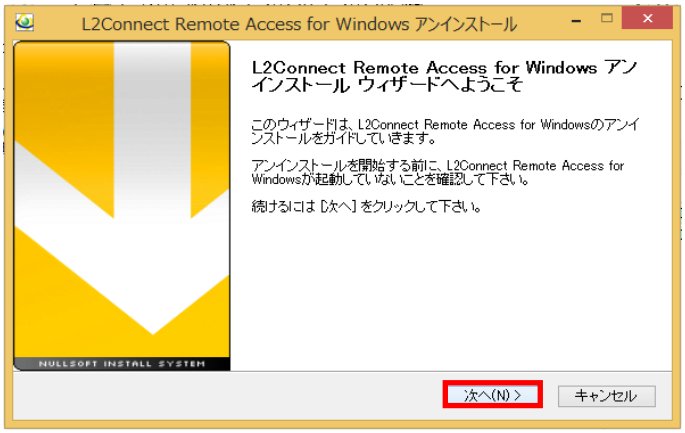
６．２　L2C クライアントのアンインストール

※管理者権限のあるユーザで実施して下さい。

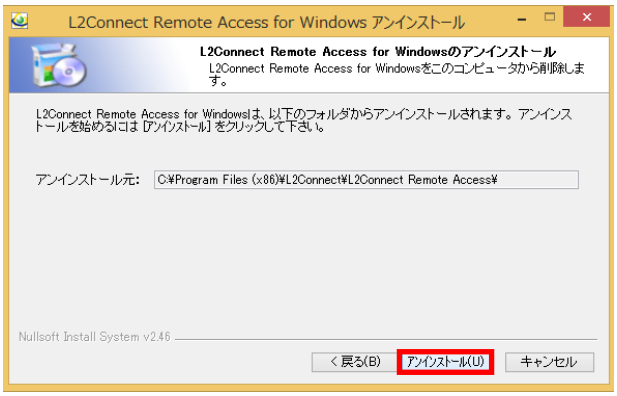
１）「３．３　L2C サーバとの接続の切断」を参照し、L2C サーバとの接続を切断して下さい。

２）「デスクトップ」－「コントロールパネル」－「プログラムと機能」を起動、「L2Connect Remote Access for Windows」を選択し、「アンインストール」をクリックしてアンインストールを実行します。

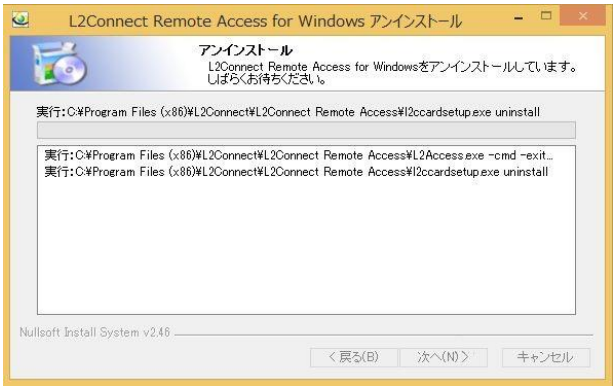
３）「アンインストールを開始する前に L2Connect Access for Windows が起動していないことを確認して下さい。」というメッセージが表示されますので、確認後「次へ」をクリックします。



4）「アンインストール」をクリックして下さい。



5）アンインストールの実行画面が表示されます。



6）アンインストールが完了したら、「完了」をクリックして下さい。

※L2C クライアントのアンインストールの場合は、コンピュータを再起動する必要はありません。

以上で、L2C クライアントのアンインストールは完了です。

６．３　アンインストール後の L2Connect 仮想ネットワークデバイス

L2C クライアントをアンインストールする場合、L2C クライアントのプログラムファイルはすべて削除され、L2Connect 仮想ネットワークデバイスも自動的に削除されます。
ただし、L2Connect 仮想ネットワークデバイスに設定されていた MAC アドレスは、コンピュータに記憶されています。
再度、L2C クライアントをインストールした場合、コンピュータに記憶されている MAC アドレスが L2Connect 仮想ネットワークデバイスに設定されます。

７．トラブルシューティング

７．１　L2C クライアントのトラブルシューティング

L2C サーバに接続する際に、エラーが発生して L2C サーバに接続できない場合は、「接続状況」画面または「ログイン」画面に表示されるエラーメッセージを参考にトラブルシューティングを行うことができます。
表示されるエラーメッセージとその対処方法を以下に示します。
以下のトラブルシューティングを実施しても問題が解決できない場合は、お客様のシステム管理者かネットワーク管理者にお問い合わせ下さい。

７．２　L2C クライアントによる接続動作時に発生するエラー

L2C クライアントによる、接続動作時に発生するエラーに対する対処方法を以下に示します。

・「仮想ネットワークデバイスが利用できません」

L2Connect の通信に使用する仮想ネットワークデバイスを利用できませんでした。
再度、L2C サーバへの接続を行って下さい。接続できなかった場合は、コンピュータを再起動してから L2C サーバに接続して下さい。

・「サービスとの接続がタイムアウトしました」

L2Connect Communication Engine との接続がタイムアウトしました。
再度、L2C サーバへの接続を行って下さい。接続できなかった場合は、コンピュータを再起動してから L2C サーバに接続して下さい。

・「サービスとの接続に失敗しました」

L2Connect Communication Engine との接続に失敗しました。
再度、L2C サーバへの接続を行って下さい。接続できなかった場合は、コンピュータを再起動してから L2C サーバに接続して下さい。

・「認証デバイスがみつかりません」

認証デバイスが見つかりませんでした。認証デバイスが正しく接続されているか確認して下さい。

・「無効な PIN コードが入力されました」

入力された PIN コードは無効です。正しい PIN コードを確認して入力しなおして下さい。

・「PIN コードの有効期限が切れています」

入力された PIN コードの有効期限が切れています。
お客様のシステム管理者かネットワーク管理者にお問合せ下さい。

・「PIN コードがロックされています」

PIN コードがロックされているため、認証デバイスを使用できません。
お客様のシステム管理者かネットワーク管理者にお問合せ下さい。

・「サーバ証明書がまだ有効ではありません」

お使いのコンピュータの日付と時刻の設定が正しいか確認して下さい。

７．３　L2C サーバへの接続時に発生するエラー

L2C サーバへの接続時に発生するエラーに対する対処方法を以下に示します。

・「ホスト名が正しくありません」または「不明なホストです」、「指定したホストまで到達できません」

接続先の L2C サーバへ指定したホスト名で接続できませんでした。
指定したホスト名が間違っている可能性があります。指定したホスト名を確認して下さい。
または DNS 設定などの名前解決方法が正しいか確認して下さい。
（L2C サーバのホスト名は USB トークンに格納されていますので、お使いのコンピュータのインターネット接続設定が正しいか確認して下さい。）
インターネット接続設定が正しい場合は、お客様のシステム管理者かネットワーク管理者にお問合せ下さい。

・「指定したホスト名及びポート番号に接続できませんでした」

接続先の L2C サーバへ、指定したホスト名とポート番号で接続できませんでした。
指定したホスト名またはポート番号が間違っている可能性があります。
指定したホスト名及びポート番号を確認して下さい。
（L2C サーバのホスト名は USB トークンに格納されていますので、お使いのコンピュータのインターネット接続設定が正しいか確認して下さい。）
問題が解決しない場合は、お客様のシステム管理者かネットワーク管理者にお問合せ下さい。

・「指定したホスト名及びポートでサーバが起動していません」

接続先の L2C サーバへ、指定したホスト名とポート番号で接続できませんでした。
指定されたホスト名及び、ポート番号上で動作しているプログラムが L2C サーバでない可能性があります。指定したホスト名及びポート番号を確認して下さい。
問題が解決しない場合は、お客様のシステム管理者かネットワーク管理者にお問合せ下さい。

・「指定したホスト名とサーバ証明書に記述されたアドレスが一致しません」

接続先の L2C サーバが提示したサーバ証明書の Common Name 項目が、サーバのアドレス（FQDN）と異なる可能性があります。ホスト名が正しく設定されているか確認して下さい。

・「サーバ証明書の有効期限が切れています」

接続先の L2C サーバのサーバ証明書の有効期限が切れているため、接続できません。
お客様のシステム管理者かネットワーク管理者にお問い合わせ下さい。

・「サーバ証明書の検証に失敗しました」

接続先の L2C サーバが提示したサーバ証明書が、L2C クライアント（接続プロファイル）に登録されている信頼する認証局によって署名されたものではないため、サーバの正当性を検証することができなかった可能性があります。信頼する認証局の認証局証明書が正しく登録されているかどうか確認して下さい。

（L2C クライアントのインストール時に接続プロファイルが読み込めていない場合、信頼する認証局の認証局証明書が正しく登録されません。）

問題が解決しない場合は、お客様のシステム管理者かネットワーク管理者にお問合せ下さい。

・「ユーザ認証に失敗しました」

接続先の L2C サーバでユーザ認証できませんでした。以下の原因が考えられます。

設定が正しく登録されているかどうか確認して下さい。

① 証明書、ライセンスが有効なものでない。
② 仮想スイッチ名の指定が間違っている。
③ 仮想スイッチにユーザが登録されていない。

（ユーザ認証に必要な情報は、USB トークンに格納されています。）

問題が解決しない場合は、お客様のシステム管理者かネットワーク管理者にお問合せ下さい。

・「ライセンスが未登録か同一ライセンスで接続中のユーザがいます」

L2C クライアントに登録されているライセンス情報（UnitID または種別）が接続先の L2C サーバの情報と一致していないため、接続できません。

または、同一のライセンスを持つユーザが別のコンピュータから L2C サーバに接続している可能性があります。

問題が解決しない場合は、お客様のシステム管理者かネットワーク管理者にお問合せ下さい。

・「サーバのセッション数上限を超えたために接続できません」

L2C サーバ側で設定されている、最大セッション数の上限値を超えた接続が L2C サーバ、または仮想スイッチに対して行われている可能性があります。お客様のシステム管理者かネットワーク管理者にお問い合わせ下さい。

・「このユーザは接続拒否されています」

L2C サーバで設定できるオプションのうち、「接続拒否」が設定されている可能性があります。お客様のシステム管理者かネットワーク管理者にお問い合わせ下さい。

・「接続先のサーバがクライアントの接続プロトコルに対応していません」

接続先の L2C サーバと L2C クライアントの接続プロトコルが一致していないため、
接続できません。お客様のシステム管理者かネットワーク管理者にお問い合わせ下さい。

・「証明書が壊れているか暗号化アルゴリズムが正しくありません」

クライアント証明書が壊れている可能性があります。または、L2C クライアントが未対応の暗号化アルゴリズムが利用されている可能性があります。お客様のシステム管理者かネットワーク管理者にお問い合わせ下さい。

・「サーバが証明書を送ってきませんでした」

接続先の L2C サーバからサーバ証明書が送付されていない可能性があります。
お客様のシステム管理者かネットワーク管理者にお問い合わせ下さい。

・「プロキシサーバに要求された認証に失敗しました」

プロキシサーバ経由での接続で、指定されたユーザ名とパスワードで認証エラーが発生し、接続できませんでした。プロキシサーバの認証情報を確認して下さい。
問題が解決しない場合は、お客様のシステム管理者かネットワーク管理者にお問い合わせ下さい。

・「プロキシエラー」

指定したプロキシサーバを経由した接続ができませんでした。プロキシサーバのサーバ名、ポート番号、認証情報の設定を確認して下さい。
問題が解決しない場合は、お客様のシステム管理者かネットワーク管理者にお問い合わせ下さい。

７．４　L2C サーバとの接続中に発生するエラー

L2C サーバとの接続中に発生するエラーに対する対処方法を以下に示します。

・「通信がタイムアウトしました」または「サーバとの通信が切断されました」、「接続中に入出力エラーが発生しました」

接続中の L2Connect 通信が、通信タイムアウトにより切断されました。再接続して下さい。現象が頻発する場合は、お客様のシステム管理者かネットワーク管理者にお問い合わせ下さい。

↓

（インターネット接続環境について）

L2Connect 通信は、L2C サーバとの接続にインターネット接続を使用しています。

そのため、インターネットへの接続方法がダイアルアップ（ISDN、PHS や 3G 等）の場合や ADSL などインターネット接続点との距離やノイズにより通信品質が影響を受けやすい場合は、「通信タイムアウト」が頻発する場合があります。

「通信タイムアウト」が頻発する場合は、お客様のシステム管理者かネットワーク管理者に調査を依頼して下さい。

L2Connect 通信をしているホストに ping を実行して、応答（Reply time）が 1000ms を超える場合は、Windows が「通信タイムアウト」を検知する可能性が高くなります。

８．SECURE CONNECT サポートサイト

８．１　SECURE CONNECT サポートサイト

SECURE CONNECT サポートサイトについては、「OPTAGE ユーザーサポート」内の以下 URL をご参照ください。

・**SECURE CONNECT**　サポート
https://support.optage.co.jp/service/secureconnect/

・**SECURE CONNECT**　約款・規約一覧
https://support.optage.co.jp/contract/stipulation.html

SECURE CONNECT Client Installation Manual ver8.0

■ 改訂履歴

2005 年 1 月 12 日 Secure Mobile クライアント インストール マニュアル ver1.00
初版

2005 年 1 月 16 日 Secure Mobile クライアント インストール マニュアル ver1.01
修正内容： 内容修正

2005 年 1 月 23 日 Secure Mobile クライアント インストール マニュアル ver1.03
修正内容： 内容修正、項目追加

2005 年 3 月 25 日 Secure Mobile クライアント インストール マニュアル ver1.10
修正内容： ＵＳＢトークン対応

2005 年 3 月 30 日 Secure Mobile クライアント インストール マニュアル ver1.20
修正内容： 項目追加

2005 年 8 月 30 日 Secure Mobile クライアント インストール マニュアル ver1.30
修正内容：内容修正、項目追加

2005 年 11 月 30 日 Secure Mobile Client Installation Manual ver2.00
修正内容：内容修正、Secure Logon 同梱廃止による項目削除、ePassNgMgr の項目追加

2006 年 7 月 10 日 Secure Mobile Client Installation Manual ver2.01
修正内容：USB トークン閉塞時の対応について追加、ユーザ PIN を忘れた時の対応について追加

2006 年 7 月 12 日 Secure Mobile Client Installation Manual ver2.02
修正内容：ユーザ PIN のリセットについて内容修正

2006 年 7 月 25 日 Secure Mobile Client Installation Manual ver2.03
修正内容：SoftEther CA Client の説明文修正、設定方法について内容修正

2007 年 2 月 6 日 Secure Mobile Client Installation Manual ver3.00
修正内容：サーバの L2Connect 移行にともなう修正、SoftEther CA Client から L2Connect Remote Access への変更

2007 年 4 月 24 日 Secure Mobile Client Installation Manual ver3.10
修正内容：クライアントソフトのバージョンアップにともなう修正、L2Connect Remote Access 1.0 for Windows から L2Connect Remote Access 1.1 for Windows への変更

2007 年 7 月 25 日　**SECURE CONNECT** Client Installation Manual　ver4.00
修正内容:サービス名を Secure Mobilel から **SECURE CONNECT** へ変更したことにともなう修正、クライアントソフトのバージョンアップにともなう修正、L2Connect Remote Access 1.1.1 for Windows の WindowsVista 対応、ePass1000 PKI ドライバー v4.2 for Windows の WindowsVista 対応、ePassNgMgr（Ver.2.1）の WindowsVista 対応

2008 年 6 月 27 日　**SECURE CONNECT** Client Installation Manual　ver4.10
修正内容：クライアントソフトのバージョンアップにともなう修正、L2Connect Remote Access 1.1.1 for Windows から L2Connect Remote Access 1.2.3 for Windows への変更

2010 年 6 月 9 日　**SECURE CONNECT** Client Installation Manual　ver4.20
修正内容：クライアントソフトのバージョンアップにともなう修正 L2Connect Remote Access 1.2.3 for Windows から L2Connect Remote Access 1.3.2 for Windows への変更、L2Connect Remote Access 1.3.2 for Windows の Windows7 対応、ePass1000 PKI ドライバー v4.4 for Windows の Windows7 対応、ePassNgMgr（Ver.2.1）の Windows7 対応

2013 年 10 月 1 日　**SECURE CONNECT** Client Installation Manual　ver4.30
修正内容：クライアントソフトのバージョンアップにともなう修正、Windows8 対応

2013 年 12 月 9 日　**SECURE CONNECT** Client Installation Manual　ver4.31
修正内容：メトリックに関する設定例を追記

2014 年 6 月 16 日　**SECURE CONNECT** Client Installation Manual　ver5.0
修正内容：Windows8.1 対応へ変更

2016 年 3 月 7 日　**SECURE CONNECT** Client Installation Manual　ver6.0
修正内容：Windows10 対応へ変更、ePass2003 対応へ変更

2016 年 4 月 4 日　**SECURE CONNECT** Client Installation Manual　ver6.1
修正内容： USB トークンドライバインストール(ePass2003)の修正

2019 年 4 月 1 日　**SECURE CONNECT** Client Installation Manual　ver6.2
修正内容： 会社再編に伴う会社名及びロゴの変更

2019 年 11 月 1 日　**SECURE CONNECT** Client Installation Manual　ver6.3
修正内容： 会社再編に伴う SECURE CONNECT サポート窓口の変更

2021 年 10 月 20 日　**SECURE CONNECT** Client Installation Manual　ver7.0
修正内容： Windows Server 2008,Windows 7 サポート終了にともなう対応 OS の変更、ePass1000, ePass1000ND 配布終了にともなう修正、PIN ブロック回数の修正、クライアントソフトのバージョンアップにともなう修正

2021 年 11 月 1 日　**SECURE CONNECT** Client Installation Manual　ver7.1

修正内容： IoT-EX 株式会社社名変更にともなう修正（旧社名：Biz Mobile 株式会社）

2023 年 1 月 6 日　**SECURE CONNECT** Client Installation Manual　ver8.0

修正内容：Windows11 サポート開始にともなう対応 OS の変更