DoMobile ASP サービス セットアップ手順

この説明書は、アクセスされる側の DoMobile PC（以下、自席 PC）に外部からアクセスするために必要なプログラムを組み込む手順を示しています。

（全ての操作は、自席 PC で実施していただきます）

※ 自席 PC にはプログラムをインストールできる権限が付与されている必要があります。詳細は管理者に御確認ください。

利用・試用期間終了後、DoMobile ASP プログラムは削除してください。

1. DoMobile CSE プログラムのインストール

① 以下の URL（注*1）へアクセスして、**プログラムを一旦ダウンロードし、デスクトップ上など任意の場所に保存してからインストールを実行**してください。ユーザアカウント制御の警告画面、警告メッセージが表示されることがありますが、「許可」または「はい」を選択して、続行してください。

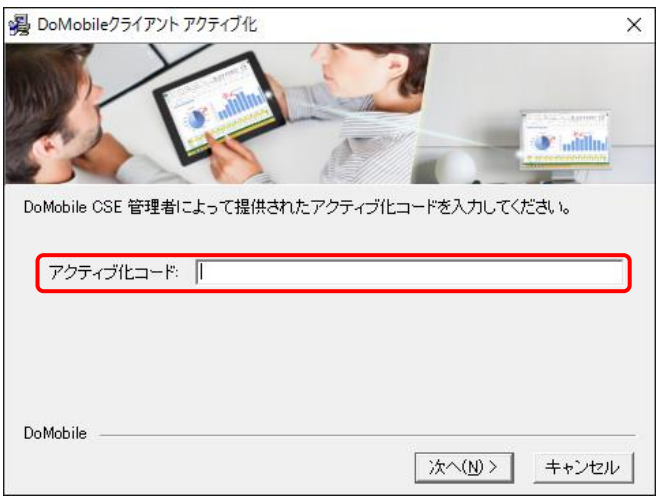
注）*1： URL については、サポートサービスセンタから展開されるアカウント発行メールに記載されている「組織コード」に従い、以下の一覧表の URL をご使用ください。
アカウント発行メールに組織コードの記載がない場合は、「[0]または[S]で始まる場合」の URL をご使用ください。

#	組織コード	URL
1	[0]または[S]で始まる場合	https://support.hitachi-solutions-create.co.jp/asp/do/pro1/dm0001setup.exe
2	[W1]で始まる場合	https://support.hitachi-solutions-create.co.jp/asp/do/pro1/dm0101setup.exe
3	[W2]で始まる場合	https://support.hitachi-solutions-create.co.jp/asp/do/pro1/dm0201setup.exe
4	[W3]で始まる場合	https://support.hitachi-solutions-create.co.jp/asp/do/pro1/dm0301setup.exe
5	[W4]で始まる場合	https://support.hitachi-solutions-create.co.jp/asp/do/pro1/dm0401setup.exe
6	[W5]で始まる場合	https://support.hitachi-solutions-create.co.jp/asp/do/pro1/dm0501setup.exe

② インストールプログラムを実行すると、インターネットからのセットアッププログラムダウンロードが開始されます。

③ ダウンロードが完了すると、アクティブ化コードの入力が要求されますので、管理者より配布された「アクティブ化コード」（数字 8 桁）を半角で入力し、「次へ>」ボタンをクリックしてください。

※ アクティブ化コード欄に値が表示される場合は、値を削除してから入力を行ってください。



第 7 版　2022 年 06 月

④ ユーザ情報を入力します。以下の要領で情報を入力して、「次へ>」ボタンをクリックします。

- 姓は最大 232 文字の半角英数字で入力してください。
- 名は最大 20 文字の半角英数字で入力してください。
- Email アドレスは最大 60 文字の半角英数字で入力してください。
- インストール先を変更する場合、**フォルダパス名に全角文字が含まれない**様にしてください。

※ これらの情報は、外部に登録/保存されることはございません。

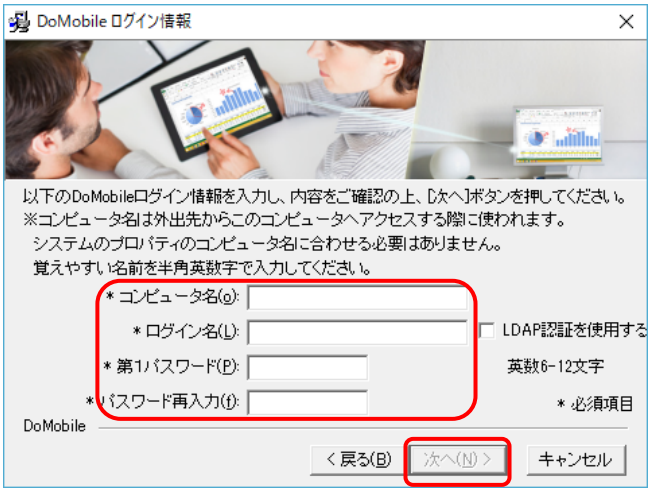
⑤ インターネット接続の画面が表示されます。「次へ>」ボタンをクリックしてください。

✧ **管理者様へ**
御使用時に設定された内容を本説明文に加筆ください。
特に指定不要で利用可能であった場合は、チェックボックスを「オフ」していただきますようご案内ください。

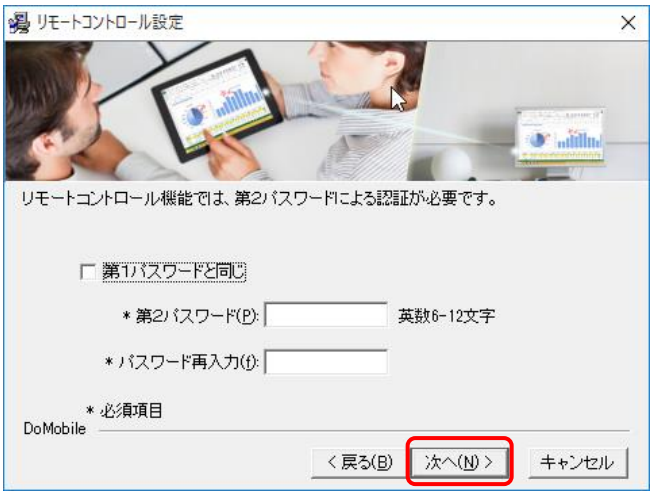
⑥ DoMobile ログイン情報は、外部から自席 PC にアクセスする際に必要となる重要な情報です。以下の要領で入力し、「次へ>」ボタンをクリックしてください。

- コンピュータ名は最大 60 文字、ログイン名は最大 64 文字、パスワードは 6 文字～12 文字の半角英数字で入力してください。
- 記号（例えば $? / @ # % ^ ~）やスペースが使用できません。
- '-'（ハイフン）は文字の間に使用できますが、先頭または末尾には使用できません。
- 例：Randy-pc-2comp は登録可能なコンピュータ名です。
- コンピュータ名とログイン名に大文字小文字の識別はありません。
- パスワードは、大文字小文字を識別します。

※ LDAP 認証を使用する場合は、項番⑧へ進んで下さい。

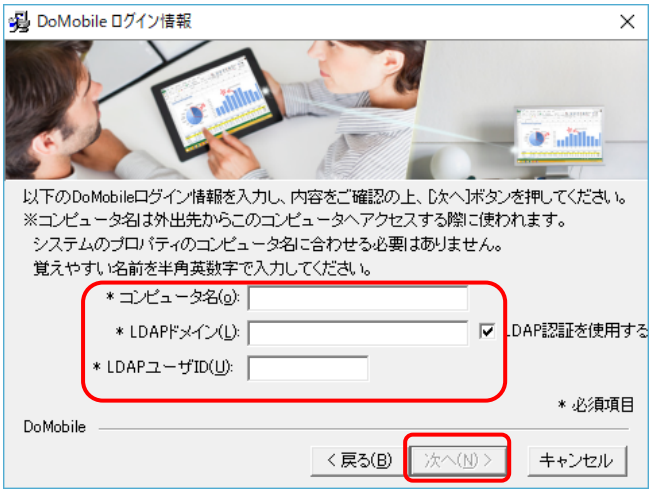


⑦ リモートコントロールの認証に必要な第 2 パスワードを以下の要領で指定し、「次へ>」ボタンをクリックします。
「第 1 パスワードと同じ」をチェックすると、第 2 パスワードの入力はできなくなり、第 2 パスワードは第 1 パスワードと同じ値になります。
チェックせず、第 2 パスワードを指定すると、第 1 パスワードと第 2 パスワードを異なる値にすることができます。



- 第 2 パスワードは、6 文字～12 文字の半角英数字で入力してください。
- パスワードは、大文字小文字を識別します。

⑧ 「LDAP 認証選択時」必要な情報を入力し、［次へ >］ ボタンをクリックしてください。

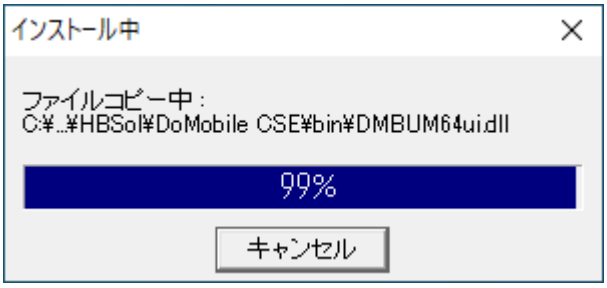


- コンピュータ名は最大 60 文字、ログイン名は最大 64 文字、パスワードは 6 文字～12 文字の半角英数字で入力してください。
- 記号（例えば $? / @ # % ^ ~）やスペースが使用できません。
- '-'（ハイフン）は文字の間に使用できますが、先頭または末尾には使用できません。
- 例：Randy-pc-2comp は登録可能なコンピュータ名です。
- コンピュータ名とログイン名に大文字小文字の識別はありません。
- LDAP ドメインは LDAP 認証を行う認証サーバの FQDN（ホスト名+ドメイン名）を入力します。
- LDAP ユーザ名はあなたの PC にログインする際に使います。

⑨ 必要なパスワードを入力し、［次へ >］ボタンをクリックしてください。ファイルのコピーが開始されます。

- LDAP ドメインは前のシートで入力した内容が自動的に入力されます。
- LDAP ユーザ名は前のシートで入力した内容が自動的に入力されます。
- パスワードは LDAP サーバの仕様に準拠します。
- Microsoft Active Directory は、LDAP サーバが Active Directory の場合にチェックオンしてください。チェックがオフの場合は OpenLDAP に準拠した方式で認証サーバに接続します。
- LDAP サーバとの通信で TLS を使用する必要がある場合は「TLS」をチェックオンしてください。その際、ポート番号が自動的に TLS 通信（STARTTLS）の標準ポートに変更されます。
- LDAP サーバとの通信で SSL を使用する必要がある場合は「SSL」をチェックオンしてください。その際、ポート番号が自動的に SSL 通信（LDAP）の標準ポートに変更されます。但し、SSL 通信を開始するために LDAP サーバが通常ポートも開放している必要があります。

⑩ 全ての情報の設定が完了すると、実際のプログラムファイルのインストールが始まります。しばらくお待ちください。



※ インストール前の自席 PC の状態によっては、インストール完了後、再起動が必要になるケースがあります。メッセージが表示されたら、「はい」ボタンをクリックして、PC を再起動してください。

インストールしたプロファイルで起動すると、登録状態や各種設定を変更するためのプログラムが起動されます。

※ 自席 PC の OS が Windows 8.1 以降の場合、ユーザアカウント制御（UAC）のメッセージが表示されます。「許可」または「はい」を選択してください。
※ UAC が OFF になっている場合、メッセージは表示されません。
※ 一般/制限ユーザで UAC が OFF の場合、「システム管理者によりこのプログラムはブロックされています・・・」が表示される場合がありますが、リモートアクセスは可能です。

⑪ 続いて以下の画面が表示されます。

- アンテナが回転中
  サーバへ登録中です。
- アンテナが赤色
  指定したコンピュータ名は、他のユーザにより既に使用されています。コンピュータ名を変更し、「適用」ボタンをクリックし、再登録を試みてください。
- アンテナが緑
  サーバへの登録が完了し、リモートアクセスができる状態になりました。
  「OK」ボタンをクリックし、画面を閉じます。

※ 二段階認証を使用する場合

「二段階認証」を有効にされているお客様は Google 認証システムを使用して、リモート端末からのアクセス時、ワンタイムパスワードによる認証が可能となります。
本機能を使用する際は、モバイルデバイスに Google 認証アプリ（Google Authenticator／Google 認証システム）（以下、Google 認証アプリ）をインストールの上、①～⑤の手順を実施してください。

※　二段階認証の有効/無効は管理者のみが管理機能（DoMobile for Manager）を使用し設定を行えます。

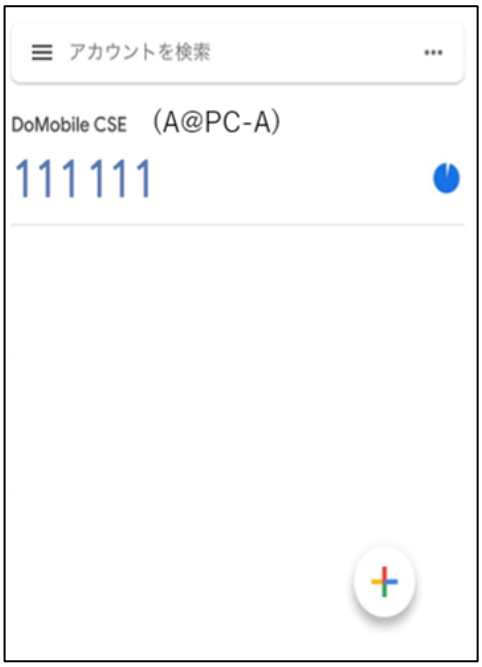
① 自席 PC に DoMobile をインストール完了後、Google 認証システム用の QR コードが自席 PC の画面に表示されます。

※　設定が完了するとこの画面は表示されなくなります。
モバイルデバイスの再設定などに備えてこの画面イメージを保管してください。
モバイルデバイスの再設定時に保存した QR コードを読み込んでいただくことで、Google 認証アプリへ再設定を行うことが可能です。（QR コードを紛失した場合は管理者へ設定の初期化を依頼してください）

② モバイルデバイスで Google 認証アプリを開き、QR コードを読み込みます。

③ QR コードを読み込むと、Google 認証アプリに Google 認証システムで使用するアカウント名（DoMobile 上で設定したユーザ名、コンピュータ名）と数字 6 桁が表示されます。

この数字 6 桁は 30 秒経つと別の数字 6 桁に変わります。



④ 自席 PC の QR コードの画面に、Google 認証アプリで表示されている数字 6 桁を入力し「完了」ボタンをクリックします。

⑤ 認証が完了すると QR コードの画面が消えます。これでリモートからのアクセス時に Google 認証システムを使用しての二段階認証が可能になります。

➢ DoMobile プログラムの再インストール時について

自席 PC に DoMobile プログラムの再インストールを行った場合は、管理者へ連絡し二段階認証の設定の初期化を依頼してください。
設定の初期化を行った場合、以前に設定した認証設定は使用できなくなりますので、再度自席 PC 上で認証の設定を行う必要があります。

- 設定の初期化は管理者のみが管理機能（DoMobile for Manager）を使用し初期化を行えます。
- 管理者の方は「ユーザーズガイド」をご確認の上、設定の初期化を行ってください。
- 管理者が設定の初期化を実施後、自席 PC の DoMobile プログラムがサーバに接続したタイミングで新しい Google 認証システム用の QR コードが自席 PC の画面に表示されますので再度、本手順書に従い設定を行ってください。
- モバイルデバイスを紛失した場合についても、管理者へ二段階認証の設定の初期化を依頼後、再度自席 PC で認証の設定を行ってください。

※ 「リモートコントロール時、この PC のモニタを隠す」について

リモートコントロール時の自席 PC のモニタを隠す機能となりますが、DoMobile ではデフォルト無効になっております。
本機能を使用される場合は、①～⑤の手順を実施いただくようお願いいたします。

自席 PC がマルチモニタ構成の場合、自席 PC の Windows のディスプレイ設定で PC 起動時にロゴマークが表示されるモニタをメインディスプレイになるように設定してください。

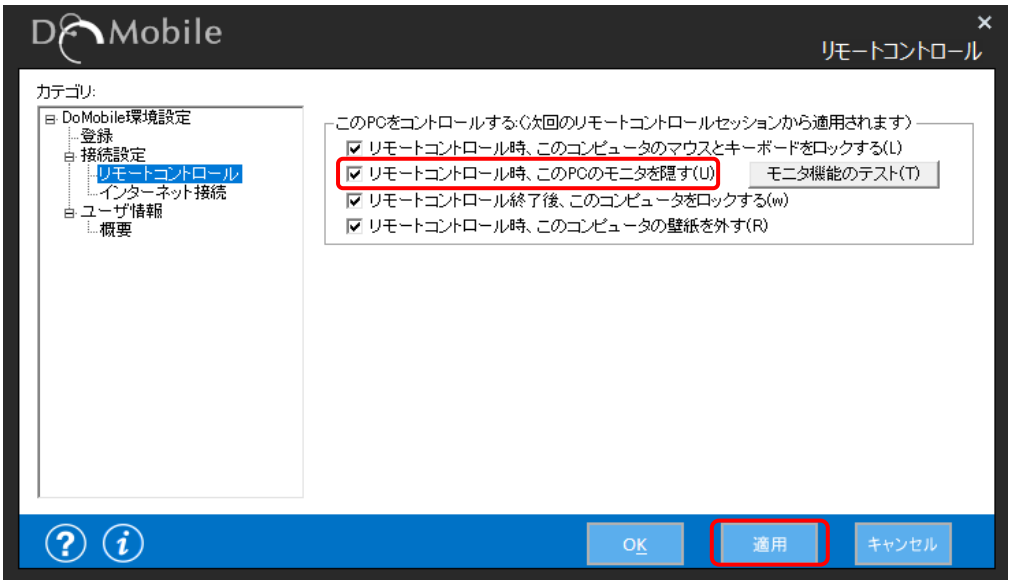
設定手順の詳細は以下の URL を参照ください。
https://support.hitachi-solutions-create.co.jp/asp/do/doc/blankscreen_man.pdf

本機能には以下の制限事項があります。

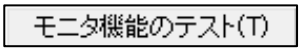
- 自席 PC がマルチモニタ構成
- リモートコントロール時の拡大率
- 自席 PC のマウスカーソル
- 自席 PC のデスクトップのアイコンの配置
- リモートコントロール中の Ctrl＋Alt＋Del
- Windows サインイン前の画面
- ユーザアカウント制御画面・セキュリティ画面
- 複数ユーザによる同時アクセス

詳細については、本手順書の【付録 1：「自席 PC のモニタを隠す機能」を使用する場合の制限事項】をご覧ください。

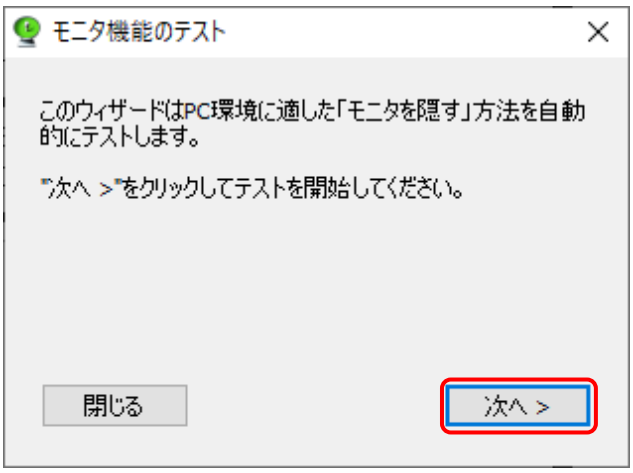
① ステータスウィンドウのカテゴリから「リモートコントロール」を選び「リモートコントロール時、この PC のモニタを隠す」をチェックオンして「適用」ボタンをクリックします。



② 「モニタ機能のテスト」ボタンをクリックします。

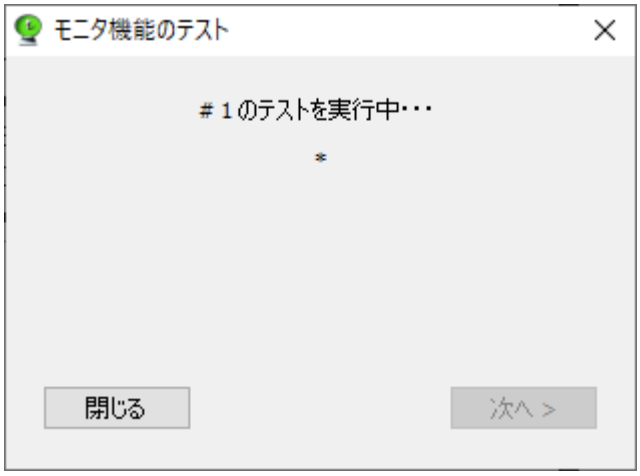


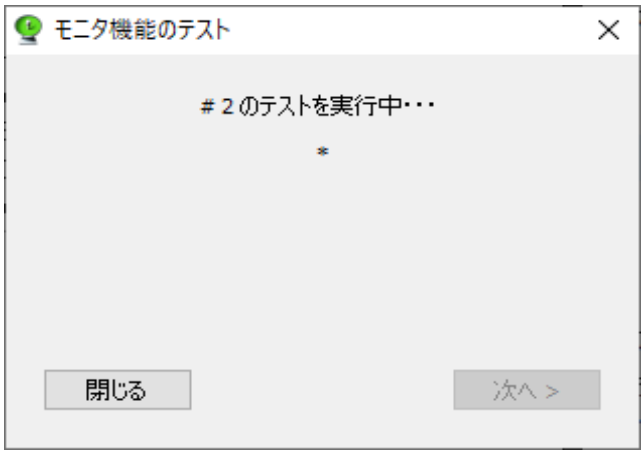
③　「次へ」ボタンをクリックします。



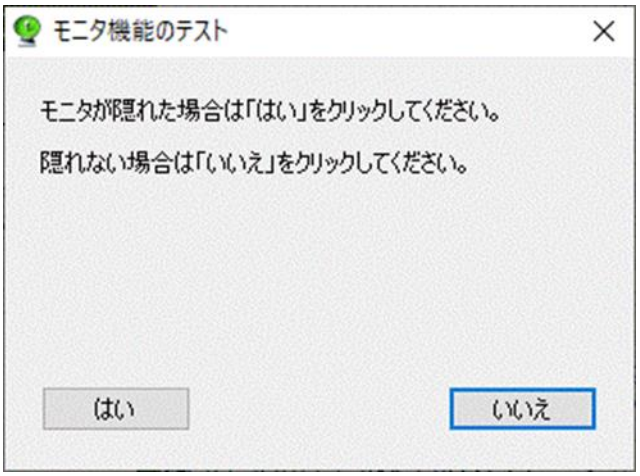
④　自席 PC の環境に適した「モニタを隠す」方法を自動でテストされます。

- 「モニタを隠す」方法は#1～＃3 まであり、最初に#1～＃2 でテストが実行されます。
- 中止する場合は「閉じる」ボタンをクリックしてください。





⑤ ＃1～＃2 でモニタが隠れた場合は、「はい」を選んでください。隠れなかった場合は、「いいえ」を選びます。「いいえ」を選んだ場合は、#3 で設定されます。



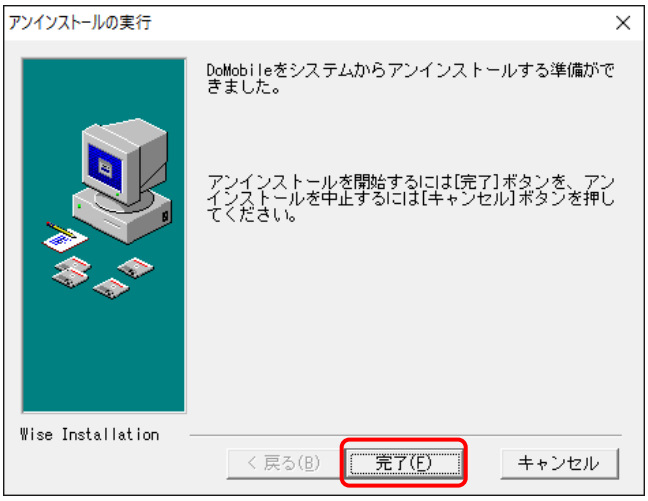
2. DoMobile プログラムのアンインストール

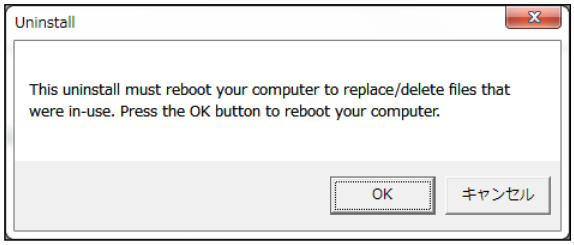
※ この作業には、再起動が必要になります。

① 「スタート」メニューを表示し、「すべてのプログラム」を選択します。

② 「DoMobile CSE」フォルダの「アンインストール」を選択します。
自席 PC の OS が Windows 8.1 以降の場合、「ユーザー アカウント制御」（UAC）が表示される可能性があります。表示された場合、「許可」または「はい」を選択してください。

③ 以下のダイアログが表示されますので、「完了」ボタンをクリック後、「OK」ボタンをクリックしてください。「OK」ボタンをクリックすると、自席 PC が再起動します。





付録 1：「自席 PC のモニタを隠す機能」を使用する場合の制限事項

- 自席 PC がマルチモニタ構成の場合
  - サポートする自席 PC のモニタ数は 2 台までとなります。

- リモートコントロール時の拡大率
  - 自席 PC の拡大率が 100%以外の場合、リモートコントロール中は強制的に拡大率が 100%に変更されます。

- 自席 PC のマウスカーソル
  - 自席 PC で他のアプリケーションなどにより標準カーソルが変更される場合、一時的にカーソルの軌跡が表示される状態になります。

- 自席 PC のデスクトップのアイコン配置
  - 環境によっては、自席 PC のデスクトップのアイコンの配置がリモートコントロール時と、リモートコントロールを行っていない時で異なります。

- リモートコントロール時の Ctrl＋Alt＋Del
  - リモートコントロール時に Ctrl＋Alt＋Del を送信した場合、一時的に自席 PC のモニタを隠す機能が解除されます。この場合は、デスクトップ画面に戻ると再度モニタを隠す機能が有効になります。
  - リモートコントロール時に Ctrl＋Alt＋Del を送信した場合、画面が更新されるまでに数秒かかります。（ご利用の環境によって、更新までの時間は異なります。）
  - リモートコントロール時に、連続して Ctrl＋Alt＋Del を送信しないでください。
  - Windows タブレットでリモートコントロール時に Ctrl＋Alt＋Del を送信した場合、以降リモートコントロールを終了するまで、リモートサウンドをご利用いただけません。

- Windows サインイン前の画面
  - リモートパワーオンや電源 ON 直後の Windows サインイン前の画面にリモートコントロールした場合、自席 PC の機種によってモニタは隠れずに表示される場合があります。この場合は、Windows にサインイン後、モニタを隠す機能が有効になります。

- ユーザアカウント制御画面・セキュリティ画面
  - ユーザアカウント制御画面、Ctrl＋Alt＋Del 押下後のセキュリティ画面にリモートコントロールした場合、自席 PC の機種によってモニタは隠れずに表示される場合があります。この場合はメッセージに応答後、モニタを隠す機能が有効になります。

- 複数ユーザによる同時アクセスについて
  - 複数のユーザが同時に同じ自席 PC へアクセスを行った場合、モニタを隠す機能が正しく動作しません。

付録 2：SAS の有効化（自席 PC が Windows Server2012,2016,2019 の場合）

リモートから Ctrl-Alt-Del を送信するため、以下の操作を行います。
ローカルキーボード操作以外で Ctrl-Alt-Del を利用した Windows ログオン操作を実施する場合には必須の設定です。

※　この設定を行わずにリモートアクセスをご利用の場合、Windows ログオン操作をスキップ、またはオフィスにいる方に Windows ログオン操作を代行してもらうことになるため、セキュリティレベルが低下する可能性があります。

①　ソフトウェアの Secure Attention Sequence の有効化
本手順は、OS が Windows 8.1 以降の場合に実施します。
（この操作をしない場合、リモートから Ctrl-Alt-Del 操作が行えません）

※　管理者様へ
本手順は、セキュリティ設定（グループポリシー）を変更するものです。エンドユーザ様に開示されるか、管理者様により実施されるかは、お客様ポリシーに依存します。
エンドユーザ様に開示しない場合は、本手順は削除してください。

②　グループポリシーエディタを起動します。
デスクトップの画面左下隅を右クリックし、「ファイル名を指定して実行」をクリックし、検索ボックスに gpedit.msc と入力してグループエディタを起動します。

③　「コンピュータの構成」→「管理用テンプレート」→「Windows コンポーネント」→「Windows ログオンオプション」→「ソフトウェアの Secure Attention Sequence を無効または有効にする」を開き「有効」を選択します。

④　「Secure Attention Sequence の生成が許可されるソフトウェアの設定」で一覧より「サービスとコンピューターの簡単操作アプリケーション」を選択します。

⑤　「OK」ボタンをクリックすることで設定が有効になります。

◆◇ユーザーズガイド◇◆
https://support.hitachi-solutions-create.co.jp/asp/domobile/webhelp/asp1/jp/getting_start.htm
◆◇よくある質問・FAQ◇◆
https://www.hitachi-solutions-create.co.jp/solution/domobile_asp/faq/index.html

以上