CLEARSURE Next

管理マニュアル

－ Ver.1.4－

ワンビ株式会社

はじめに

このたびは、CLEARSURE Next をご利用いただき、ありがとうございます。
このマニュアルは、CLEARSURE Next（以降、本サービス）の機能概要、クライアントプログラムのインストール方法、管理サーバーの設定方法および操作方法など、本サービスを効果的かつ安全にご利用いただくための重要な情報について説明しています。よくお読みになり、理解されたうえで本サービスをご利用ください。

■パソコンを紛失した場合、消去命令を発行するためには以下の項目が必要となります。
万一に備えて、これらを事前に確認しておくことをおすすめします。

- ✓ **紛失時にどのパソコンから管理サーバーにアクセスするか**
- ✓ **管理サーバーの URL　https://tdcs.trustdelete.biz/**
- ✓ **管理サーバーにログインするための ID とパスワード**

本ドキュメント内の機能名称または図は製品のバージョンにより実際の名称またはデザインと異なる場合があります。

TDCS20241225

目次

CLEARSURE Next とは

■サービス概要

本サービスは、富士通クライアントコンピューティング株式会社が提供する CLEARSURE 対応の法人向けノートパソコン、またはタブレットパソコン（以降、パソコン）の盗難・紛失対策を目的とするセキュリティソリューションです。CLEARSURE 対応のパソコンは、専用の通信モジュールを内蔵しており、パソコンの盗難／紛失が発覚したときに、管理者のパソコンから紛失したパソコンを 3G/LTE/5G 回線で遠隔操作することで、対象のパソコンにロックやデータ消去を指示できます。近年多発しているパソコンの盗難・紛失による情報漏えいに対して、万一の際に大事な情報資産の流出を未然に防ぐことが可能です。
また、管理サーバーで設定した監視ポリシーに基づいてパソコンの挙動や使用状態を常時監視し、ポリシーに違反する動作を検出した場合にパソコンのロックや強制シャットダウンを実行するなど、不正持出しの防止、不正利用の防止にも効果的です。

■主な機能

◆ データ消去

パソコンの盗難・紛失時や廃棄時にリモート指示により eMMC の上書き消去および暗号化機能付 HDD/フラッシュメモリディスクの暗号鍵を消去することにより、保存されたデータを復元できなくする機能です。通信モジュールの通信圏内であれば、対象となるパソコンの電源がオフの状態であっても、命令を受信しドライブ全体を消去することが可能です。

◆ リモートロック機能

管理サーバーからロック命令を送信することで、紛失したパソコンを操作不能にする機能です。通信モジュールの通信圏内であれば、対象となるパソコンの電源がオフの状態であっても、命令を受信し BIOS によるロックを行うことでパソコンを操作できない状態にすることが可能です。ロックされたパソコンは管理サーバーからロック解除命令を送信することでのみ、解除が可能です。

◆ ビープ機能

リモートロックの発動時に、ビープ（警告音）を鳴らして、発見を促す機能です。パソコンが建物内で行方不明になった場合などに便利です。旧モデルなど一部機種ではご利用になれません。

◆ ポリシー監視ロック機能

あらかじめ設定した監視ポリシーに違反した場合、入力デバイスをロックすることでパソコンを操作不能にします。

◆ 適正消去実行証明書発行機能

パソコンの廃棄やリースアップの際に、パソコンに保存されたデータを消去したうえで、第三者機関「データ適正消去実行証明協議会（略称 ADEC）」が発行する「データ適正消去実行証明書」を取得、閲覧することが可能です。

◆ PC 情報の取得

パソコンのハードウェア情報や OS 情報、ネットワーク情報を取得して表示することができます。また、インシデント発生時の位置情報を GPS または無線 LAN のアクセス情報から特定することができます。 ※ご利用にはハードウェアの制限があります。

◆ パソコン一括管理

複数のパソコンでご利用の場合、管理サーバーから、すべてのパソコンの消去実行や消去履歴、動作設定を一括で管理することが可能です。

■システム動作環境

クライアントプログラム対応 OS
Microsoft Windows 11 (Windows 11 Pro, Windows 11 Enterprise)
Microsoft Windows 10 (Windows 10 Pro, Windows 10 Enterprise)

ハードウェア
CPU:1GHz 以上を推奨 (ARM アーキテクチャーには対応しておりません)
メモリ(RAM): 2GB 以上を推奨
100MB 以上のハードディスク空き容量
富士通クライアントコンピューティング株式会社製 CLEARSURE 対応機種 *1
(https://jp.fujitsu.com/platform/pc/product/related/security/data_sec.html を参照)
*1 CLEARSURE 非対応機種の場合、データ消去・リモートロック機能等を除く一部の機能のみご利用可能です。

管理サーバー アクセス環境
Microsoft Edge、Google Chrome

■CLEARSURE Next のご利用にあたっての注意事項

- 1つのパソコンで CLEARSURE 3G/LTE と CLEARSURE Next を同時に利用することは出来ません。CLEARSURE 3G/LTE でご使用のパソコンを CLEARSURE Next で利用する場合は、必ず CLEARSURE 3G/LTE でディアクティベーションを実施してから CLEARSURE Next のクライアントプログラムをインストールしご利用ください。
- CLEARSURE Next では CLEARSURE 3G/LTE のディアクティベーションは行えません。CLEARSURE 3G/LTE でディアクティベーションが実施されていない場合、メーカー修理が必要になる場合があります。
- 暗号化機能付 HDD もしくは暗号化機能付フラッシュメモリディスク及びフラッシュメモリ(eMMC 以外を搭載されている場合はデータ消去機能をご利用できません。
- データ消去機能とは暗号化機能付 HDD/フラッシュメモリディスクにおいては、暗号化されたデータを復号するための暗号鍵を消去することにより、当該 HDD/フラッシュメモリディスクに保存されたデータを復元できなくするものです。フラッシュメモリ(eMMC)搭載モデルにおいては、全領域の上書き消去になります。なおフラッシュメモリ(eMMC)搭載モデルではデータ適正消去実行証明書を発行することは出来ません。
- 当該「データ消去」機能は、当該 HDD/フラッシュメモリディスク上の暗号化されたデータを消去するものではありません。
- セキュリティ強度を上げるために BIOS メニューにて管理者用パスワード、ユーザー用パスワード、HDD パスワードの設定を実施いただくことを推奨いたします。
- 結果返信には SMS での送信が行われます。この通信料金についてはお客さま負担となります。料金につきましてはお客さまのご契約を確認願います。
- 一度発行した「消去命令」「ロック命令」「ロック解除命令」「ビープ＆ロック命令」は取り消す事ができません。
- 操作の対象となるパソコンが以下の状態の場合は、「消去命令」「ロック命令」「ロック解除命令」「ビープ＆ロック命令」を受信することができません。
  - 無線通信機能の電波を停止する設定になっている場合
  - 通信エリア外またはエリア内の電波の届かない場所にある場合
  - バッテリが切れている場合
  - バッテリが取り外されている場合
  - SMS が利用できるデータ通信契約を有する SIM カードが未挿入の場合
  - SIM カードが取り換えられた場合

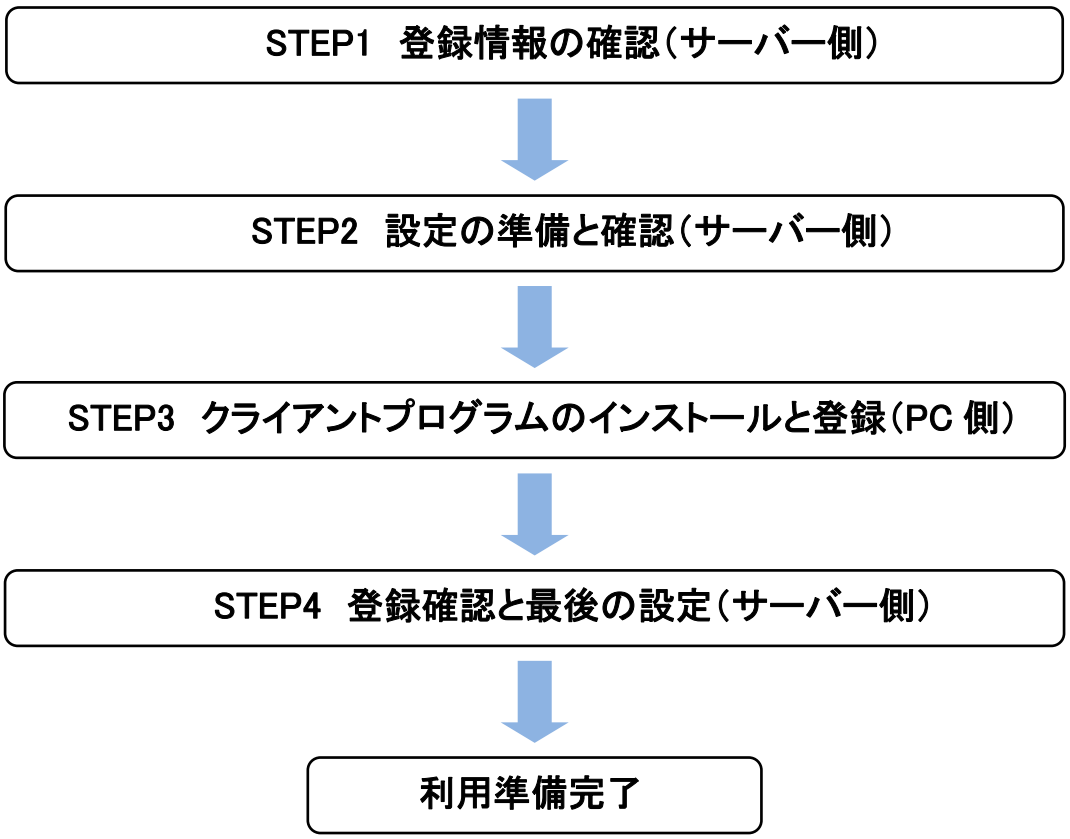
- 操作の対象となるパソコンが以下の状態の場合は、「消去命令」「ロック命令」「ロック解除命令」「ビープ＆ロック命令」の受信または処理結果が応答できない可能性があります。
  - 周囲で大量の通信が行われている、または回線の輻輳により良好な通信ができない場合
  - 金属製の鞄に入れている場合など、通信が遮断され良好な通信ができない状態にある場合
  - 通信エリア内であっても電波の届きにくい場所にある場合
  - パソコンの動作保証条件に満たない環境の場合
  - 電気通信事業者の通信網に障害が発生している場合
  - APN が正しく設定されていない場合
- パソコンの Windows OS をボリュームライセンスメディアから再インストールした場合は、各種ドライバのインストールが必要です。OS のハードウェア情報で「不明なドライバ」が存在している場合の動作は保証されませんのでご注意ください。詳細はハードウェアに添付されているインストールガイドを参照ください。
- パソコンがロックの指示を受信した場合、対象となるパソコンの動作状況に関係なく再起動します。そのため指示を実行した際の状況によっては、以下の問題が起こる可能性があります。
  - ロック解除後にパソコンが正しく起動しない
  - 作成中のデータが破壊される
  - HDD に保存されたデータが破壊される
- リモートによる消去を行う前に HDD／フラッシュメモリディスクが抜かれた場合は、消去することはできません。
- 位置情報は、パソコン内蔵の GPS を利用して取得されます。
  GPS の電波が受信できない環境の場合は、位置情報は取得できません。
- 2022 年以前に発売された機種など、一部機種ではビープ機能をご利用になれません。
- 操作の対象となるパソコンの状態により「消去命令」「ロック命令」「ロック解除命令」「ビープ＆ロック命令」の発行が出来ないことによるお客様の損害については一切保証しません。
- 以下の状況により「消去命令」「ロック命令」「ロック解除命令」「ビープ＆ロック命令」の発行ができない場合、それによるお客様の損害については一切保証しません。
  - 操作対象となるパソコンが故障を含め「消去命令」「ロック命令」「ロック解除命令」「ビープ＆ロック命令」の受信が不可能な状態にある場合
  - 無線および有線の通信網の障害により「消去命令」「ロック命令」「ロック解除命令」「ビープ＆ロック命令」の送信ができない場合
  - サーバーメンテナンス、不測の事故および第三者の攻撃によるシステムダウンにより、管理サーバーの操作ができない場合
- SIM に設定している PIN コードを間違えて入力した場合、データ消去機能、リモートロック機能、ビープ機能はご利用になれません。
- PIN コードを間違えたまま OS の再起動を繰り返した場合 PIN ロックがかかります。PIN ロックがかかった状態では、データ消去機能、リモートロック機能、ビープ機能はご利用になれません。
- PIN ロックの解除は、PIN ロック解除コードを入力するか、ご契約の通信事業者の窓口にご相談ください。
- PIN ロック解除コードを入力する方法は、購入されたパソコンの取扱説明書をご参照ください。
- PIN コードを設定しない状態でアクティベーションした後に、SIM に PIN コードを設定する場合や、設定済みの PIN コードを変更する場合は、再アクティベーションが必要です。クライアントプログラムのアンインストールを実施した後に、PIN コードを設定し、再度、クライアントプログラムのインストールと登録処理を行ってください。
- SIM をパソコンに挿入した状態で登録作業を行ってください。登録作業については「第１章 STEP3 クライアントプログラムのインストールと利用登録」をご参照ください。
- 法人向けパソコン・タブレット製品情報ページのドライバダウンロード（https://www.fmworld.net/biz/fmv/index_down.html）に最新の BIOS、ファームウェアが提供されているかどうかをご確認いただき、提供されている場合は最新版を適用してください。

- 国際 SMS が利用できるデータ通信契約が必要です。FENICS Ⅱ ユニバーサルコネクトで提供するモバイル回線、または NTT ドコモ、au、ソフトバンクの通信サービスが利用できます。また、他の通信事業者を利用する場合は、国際 SMS が利用できることを通信事業者にお問い合わせの上、事前に動作することをご確認ください。
- CLEARSURE Next は、情報漏えいの防止に対して 100%保証するものではありません。
- データ消去を実行した後に、機器を再セットアップするには 9.1 項をご参照ください。 正しい手順で再設定が行われないと、メーカー修理が必要となる場合があります。
- ロック後のパソコンの故障や SIM カード不具合によりロックの解除が行えなくなった場合は、メーカー修理が必要となる場合があります。
- パソコンを修理に出す場合は、事前に必ず CLEARSURE Next クライアントプログラムをアンインストールしてください。修理完了後に再度 CLEARSURE Next クライアントプログラムのインストールおよび 登録処理を実施してください。パソコンが起動できない状態など、修理に出す前にクライアントプログラムのアンインストールができない状態の場合は、修理完了後に必ずクライアントプログラムのアンインストールと再インストール、再登録処理を実施してください。

※ クライアントプログラムは、1 つのライセンスにつき、1 つの OS にインストールできます。
※ 必要メモリ容量、およびハードディスク容量は、システム環境によって異なる場合があります。
※ クライアントプログラムをお使いになる前に、使用許諾契約書を必ずお読みください。
※ 本サービスの仕様は予告なく変更される場合があります。
※ パソコンの登録、プログラムのダウンロード、管理サーバーの閲覧などのご利用には、インターネット接続環境が必要です。

1．基本セットアップ

本サービスをご利用になるにはまず以下の 4 つのステップに沿って管理サーバーとパソコン側のクライアントプログラムのセットアップが必要です。



STEP 1　登録情報の確認

※以下の作業はインターネット接続が必要です。

1. WEB ブラウザ（Microsoft Edge など）で次の URL にアクセスし、管理サーバーにログインします。
   https://tdcs.trustdelete.biz/ ※事前にログイン ID とログインパスワードをご用意ください。ログイン ID と初期パスワードはサービス利用開始案内書に記載されています。

2. ログイン後、上部メニューから ADMIN 画面を開き、運用に必要な情報を事前に確認します。

① ログイン ID：ログイン ID の変更が必要な場合、管理者のメールアドレスなどを入力し、画面下部の**[保存]**ボタンをクリックします。
② ログインパスワード：管理者用のログインパスワードを変更する場合、ここで新しい値を入力し**[保存]**ボタンをクリックします。
③ グループ ID：管理対象のグループを変更する場合、ここで対象グループを選択し**[保存]**ボタンをクリックします。グループの作成方法は「5.2 グループの作成」を参照してください。
④ 権限：管理者の権限を変更する場合、ここで権限を選択し**[保存]**ボタンをクリックします。権限の詳細については「5.1 管理者権限とユーザー権限」を参照してください。

⑤ シリアル番号：パソコンの登録時に必要な 8 桁のシリアル番号です。
⑥ 更新月：ご契約の更新月が表示されます。
⑦ 消去証明書発行可能数：データ適正消去実行証明書の発行可能枚数が表示されます。
⑧ 契約台数：ご契約いただいた台数が表示されます。
⑨ 登録台数：すでに管理サーバーに登録済のパソコンの台数が表示されます。
⑩ 管理者のメールアドレスを登録します。メールアドレスは最大2つまで登録出来ます。登録されたメー

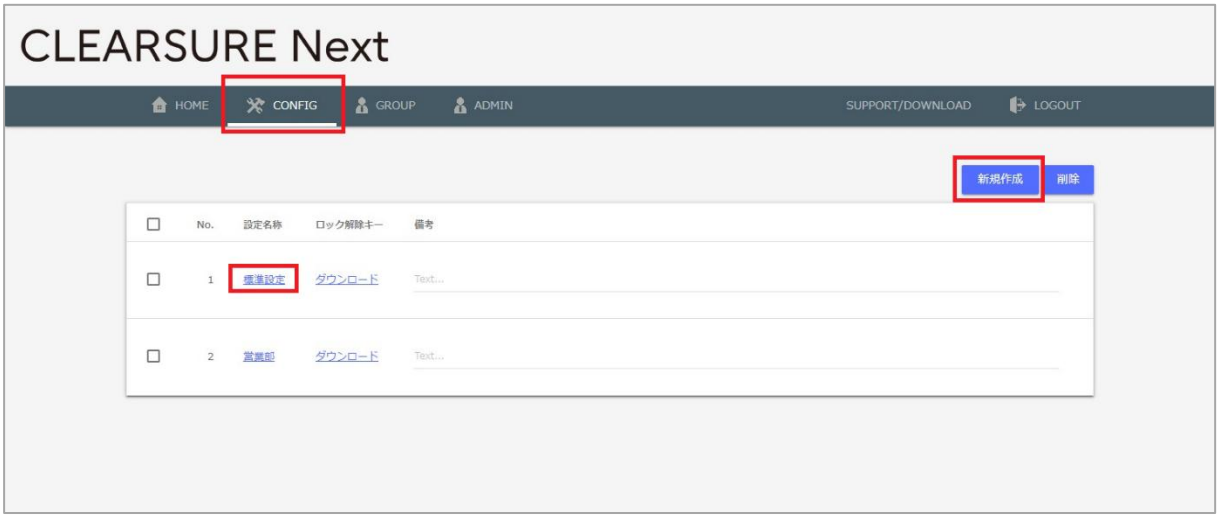
ルアドレスにはパソコンの登録完了時、消去完了時にメール通知が行われます。

※注意	・各項目を変更した場合、必ず**[保存]**ボタンをクリックしてください。
※ヒント	・初期パスワードは速やかに変更することを推奨します。 変更したパスワードは忘れないように安全な方法で保管管理してください。 ・ログイン ID は、4～32 文字の半角英数文字および記号がご利用できます。 ・ログインパスワードは、4～32 文字の半角英数文字および記号がご利用できます。

STEP 2　設定の準備と確認

ここではクライアントプログラムの動作を決める監視ポリシーメニューについて説明します。

管理サーバーにログイン後、上部のメニューから CONFIG 画面を開き、画面右上の**[新規作成]**ボタン、または登録済みのポリシーの**[設定名称]**をクリックしてポリシーの編集ページを表示します。
監視対象となるパソコンの用途に応じて適切な監視ポリシーを設定して保存してください。最大で 10 個の監視ポリシーを作成・保存することが可能です。



※ヒント	・パソコンの利用場所や利用者の所属部署に応じて異なる監視ポリシーを作成することができます。 ・どのパソコンにどのポリシーを割り当てるかは HOME 画面で自由に選択することができます。登録直後は No.1 のポリシーが適用されます。

設定内容

① 設定名称
設定に 30 文字以内でオリジナルの名称を付けることができます。この名称が HOME 画面の設定名称に表示されます。

② アンインストールパスワード
メインプログラムが不正にアンインストールできないようにパスワードで保護することができます。4 文字以上 32 文字以内の半角英数字でパスワードを指定します。

③ ロック解除キー
ポリシー違反でロックされたパソコンを解除するためのキーを設定します。4 文字以上 32 文字以内の半角英数字を設定してください。解除キーの使用方法は「3.2 ポリシー違反によるロック」を参照してください。

④ 備考
監視ポリシーの説明等を必要に応じて 500 文字以内で入力してください。

ネットワーク関連ポリシー

⑤ オンライン／オフラインの監視
パソコンがオフラインになるとロックを実行します。通常はオンラインでご利用になるパソコンに適しています。有線・無線接続に関わらずパソコンがオンラインの時にロックは発動しません。

⑥ ネットワークの接続先監視
指定したゲートウェイ以外の接続を検出した時にパソコンをロックします。許可するゲートウェイアドレスは最大 3 個まで指定可能です。パソコンがオフラインの状態では発動しません。

※ヒント	入力欄には IP アドレスを指定してください。複数入力する際はカンマで区切ります。

⑦ 無線 LAN のアクセスポイント監視
指定した無線 LAN アクセスポイントの SSID を、タイマーで指定した時間以上検出できない状態が続いた場合にパソコンをロックします。指定時間内に 1 度でも指定の SSID を検出するとタイマーが

リセットされゼロからカウントを再開します。指定済みの SSID の電波を検出することができればアクセスポイントに接続する必要はありません。タイマーは 0 から最長 24 時間まで 8 種類から選択できます。パソコンがシャットダウンまたはスリープされている状態でもタイマーのカウントは進行します。

※注意	・Windows 11 2024 Update（Windows 11, version 24H2）にて本機能をご利用いただく場合は、Windows の「設定」から「プライバシーとセキュリティ」＞「位置情報」の「位置情報サービス」をオンにしてください。

⑧ 無線 LAN 接続の制御

無線 LAN 経由のインターネット接続の可否を 2 つの方法でコントロールします。

■指定の SSID 以外への接続を禁止：⑨のテキストボックスで指定した SSID 以外の無線 LAN の使用を禁止します。禁止された無線 LAN への接続を検知すると即座に切断します。

■すべての Wi-Fi 接続を禁止する：無線 LAN への接続ができなくなります。

本機能により無線 LAN 接続を切断する場合は、警告メッセージが表示されます。

⑨ 許可する無線 LAN の SSID

上記⑦または⑧の機能で利用する無線 LAN アクセスポイントを指定します。

⑦無線 LAN のアクセスポイント監視機能	ここに入力指定した SSID を時間内に検出できない場合、セキュリティアクションを実行します。
⑧無線 LAN 接続の制御機能	ここに入力指定した SSID 以外の接続をすべて禁止します。
利用できる SSID	英数字および記号のみ使用できます。 アスタリスク（＊）、カンマ、および日本語などのダブルバイトを含む SSID は使用できません。

※ヒント	・文字制限に使用できない SSID が含まれる場合はアクセスポイントの SSID を変更してご利用ください。 ・SSID は最大 10 個まで指定できます。複数指定する際はカンマで区切ります。

SIM の監視

⑩ SIM カードの監視

無線 WAN（5G/LTE/3G モジュール）搭載機種において、SIM カードが認識できない時にパソコンをロックします。無線 WAN が搭載されていない機種では、監視を有効にしてもロックは発動しません。

コンピューターの利用エリア監視

⑪ コンピューターの位置情報の監視

パソコンがあらかじめ指定した利用エリアから外に出た時にパソコンをロックします。利用エリアは中心点を緯度・経度で指定し、その中心点からの半径を 1km から 10km の間で指定します。社内や施設内など利用エリアが明確に制限されているパソコンに適しています。最大 4 か所のエリアを設定することができます。

利用エリアの指定方法
[位置情報設定]ボタンをクリックして地図画面を開きます。必要に応じて地図をドラッグまたは拡大／縮小して位置を調整します。許可範囲は地図の上にあるスライドバーで調整します。位置と範囲が決まったら**[中心の位置に設定]**ボタンをクリックした後、右下の**[保存]**ボタンをクリックすると位置情報が保存されます。

ロックのポリシー

⑫ 操作ロック実行中の画面表示
ロックの実行時にパソコンにロック画面を表示できます。ロック画面には大小 2 つの任意のメッセージを挿入できます。

※注意	・ご利用の環境によっては、操作ロックの実行中にロック画面が表示されずに黒い画面や Windows にログオンする前の画面などが表示されることがあります。ロック画面が表示されない場合でも操作ロックの動作中は入力デバイスが無効化されているため、パソコンの操作は不可能です。 ・ロック命令（3 項参照）によるロック発動時には、BIOS によるシステム固定のメッセージが表示されます。
※ヒント	・メッセージ 1(大)は最大 50 文字、メッセージ 2（小）は最大 75 文字入力できます。 ・メッセージを表示するにはメッセージ 1（大）の入力が必須です。メッセージ 2（小）のみを表示することはできません。 ・ロックが発動するとロック画面の中央部（メッセージのすぐ下）に発動要因となったポリシーが小さく英文で表示されます。

Windows ログオンパスワードの監視

⑬ Windows ログオンパスワードの監視
Windows ログオン時にパスワードを一定回数連続して間違えた時にパソコンを強制シャットダウンします。パスワードの入力失敗回数は 3 回から 10 回の間で指定できます。
※注意　本ポリシーに違反した時のアクションは強制シャットダウンのみです。他のポリシーのようにロックアクションを選択・実行はできません。

以上すべての設定が完了したら、画面の右下にある**[保存]**ボタンを必ずクリックしてください。

※注意	**[保存]**ボタンを押すまで設定項目は保存されません。
※ヒント	・本サービスでは最大 10 個の監視ポリシーを作成できます。複数のパソコンに異なる監視ポリシーを割り当てる場合は同様の操作で 2 個目以降のポリシーを作成してください。

STEP 3　クライアントプログラムのインストールと登録

1. 本サービスで、データ消去機能、リモートロック機能、ビープ機能を利用するためには、管理対象のパソコンに以下のドライバ、ファームウェアがインストールされている必要があります。
富士通法人向けパソコン・タブレット製品情報ページのドライバダウンロード（https://www.fmworld.net/biz/fmv/index_down.html）に最新の BIOS、ファームウェアが提供されているかどうかをご確認いただき、提供されている場合は最新版を適用してください。ドライバのインストール方法については、ハードウェア本体マニュアルの製品ガイド内のソフトウェア、インストールの項目を参照ください。
    - Fujitsu BIOS Driver
    - FUJ02E3 Device Driver
    - FUJ0430/FUJ0420 デバイスドライバー
    - LAN/WAN : Sierra Wireless WWAN Driver または Thundercomm Mobile Broadband INF Package

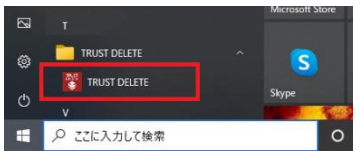
    ※機種によっては以下のドライバのインストールが必要となります。
    - 富士通拡張機能ユーティリティ

2. 管理サーバーにログインして上部のメニューから SUPPORT/DOWNLOAD 画面を開きます。

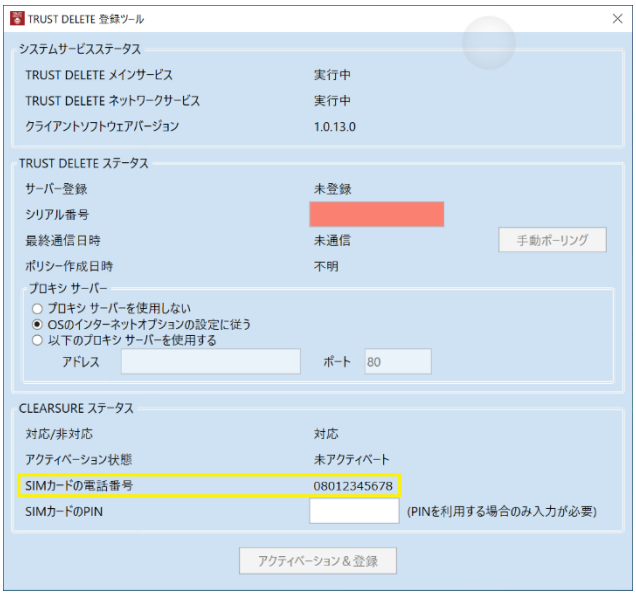
3. 別ウインドウでサポートページが開いたら、CLEARSURE Next プログラムのダウンロードの[こちらからダウンロード]をクリックしてプログラムを管理対象のパソコンに保存します。

4. 管理対象のパソコン上で、取得したプログラム（TDCSInst.exe）をダブルクリックし、ウィザードに従ってインストールしてください。インストール後は再起動が必要です。

5. 管理対象のパソコンに SMS の送受信が可能な SIM カードを挿入もしくは eSIM の有効化を行い、通信ができることを事前に確認してください。パソコンを起動し、機内モードがオン、携帯ネットワークがオフに設定されていないことを確認したら、プログラムメニューから**[TRUST DELETE]**を実行してください。



6. TRUSTDELETE 登録ツールが起動したら、SIM カードの電話番号が表示されていることを確認してください。電話番号が表示されない場合、パソコンが SIM カード/eSIM を認識できていない可能性があります。その場合、一旦パソコンをシャットダウンし、SIM カードを再度挿入しなおすなどして、手順 5 からやり直してください。

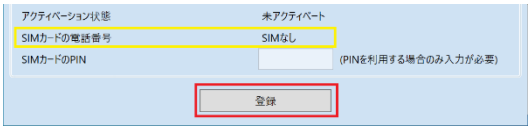


※注意	SIM が認識できない状態で以降の手順を進めた場合、データ消去機能、リモートロック機能、ビープ機能はご利用になれません。

7. シリアル番号欄に STEP1 の⑤で確認した 8 桁のシリアル番号を記入し、必要に応じてプロキシサーバーの設定の変更および、SIM カードの PIN を入力してください。

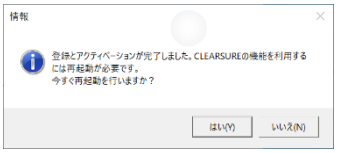
※注意	・SIM に設定している PIN コードを間違えて入力した場合、データ消去機能、リモートロック機能、ビープ機能はご利用になれません。 ・間違った PIN コードが入力されたままの状態で OS の再起動を繰り返した場合 PIN ロックがかかります。PIN ロックがかかった状態では、データ消去機能、リモートロック機能、ビープ機能はご利用になれません。

8. 必要な情報を入力したら、**[アクティベーション＆登録]**ボタンをクリックして利用登録を行ってください。
SIM カードを挿入していない場合や SIM カード/eSIM が認識できない場合などは、**[アクティベーション＆登録]**ボタンに代わり **[登録]**ボタンが表示されます。



※ヒント	・「アクティベーション」とは、BIOS 上で提供される「データ消去」「ロック」「ビープ」などのセキュリティ機能を利用可能な状態にするための処理です。アクティベーションが正常に完了していないパソコンでは、「データ消去機能」「リモートロック機能」「ビープ機能」をご利用になれません。 ・「登録」とは、管理対象のパソコンの情報を管理サーバーに登録し、制御可能な状態にするための処理です。登録が正常に完了していないパソコンは、すべての機能がご利用になれません。

9. 「登録とアクティベーションが完了しました。CLEARSURE の機能を利用するには再起動が必要です。」と表示されたらパソコンを再起動してください。
「登録が完了しました。」と表示された場合、再起動は不要です。



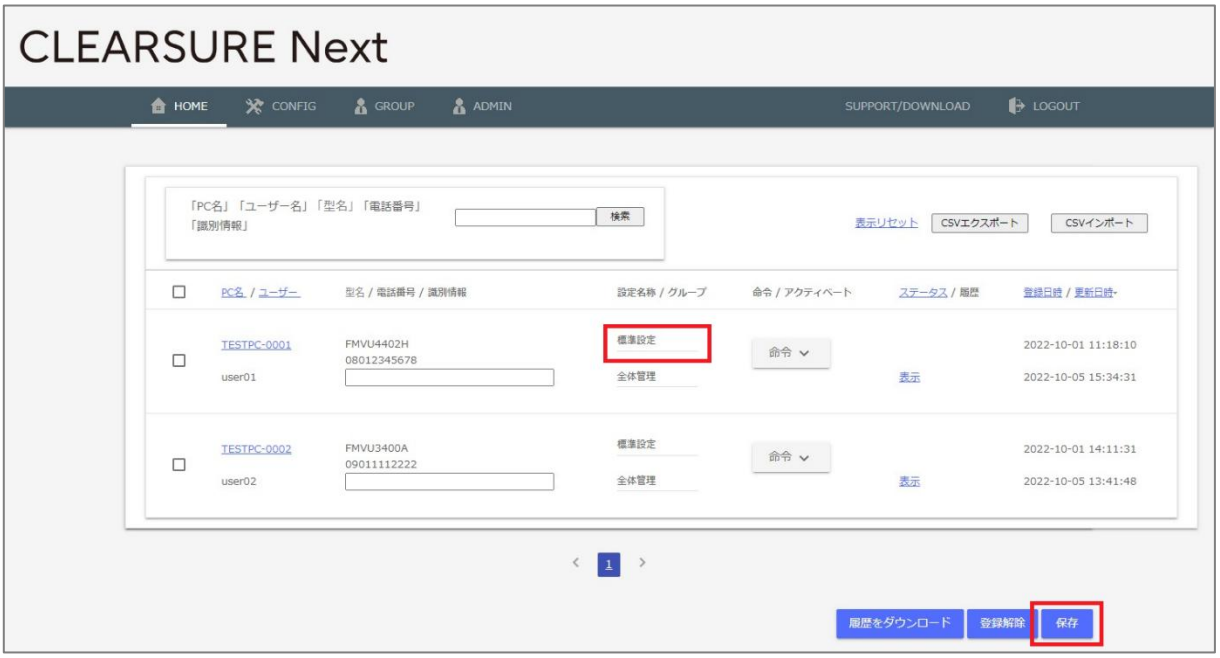
以上でクライアントの利用準備は完了です。

※注意	・インストール完了後、およびアクティベーション完了後は必ずパソコンを再起動してください。 ・登録を完了しなければ本プログラムは正しく動作しません。必ず登録を行ってください。

STEP 4　登録確認と最後の設定

ここではご利用前の最後の設定を説明します。重要なので必ず確認してください。

1. 管理サーバーにログインして HOME 画面を開きます。
2. 登録したパソコンがリストに表示されていることを確認してください。
   各パソコンの**[設定名称]**に適切なポリシー名が割り当てられているか確認してください。初期状態ではすべてのパソコンに同じ設定（設定番号1）が適用されています。パソコンごとに異なるポリシーを利用する場合はプルダウンから任意の設定名を選択してください。設定変更を適用するには必ず画面右下の**[保存]**ボタンをクリックしてください。



以上で CLEARSURE Next のご利用準備は完了です。次項からの機能詳細説明をご確認の上、お客さまにて必要な対策をご検討頂き、必要に応じて STEP2で実施した設定を見直してください。
実際の運用においては、万一の事故発生時に備え、利用者に対して、事故発生時の対処方法や報告先などを周知・徹底し、速やかに消去命令やロック命令を発行できるような意識付けをしておくことが重要です。

※注意	・管理サーバーで設定を変更しても、直ちにその設定がクライアントプログラムに反映されるわけではありません。新しい設定が反映されるためにはクライアントプログラムが管理サーバーと通信を行う必要があります。 管理サーバーで設定を変更した場合、TRUSTDELETE 登録ツールの[手動ポーリング]ボタンをクリックして最新の設定を取り込むことをおすすめします。
※ヒント	・盗難・紛失などのインシデントが発生した際に、対象のパソコンを特定しやすくできるように、パソコンの管理番号や、利用者を特定するための情報を「識別情報」欄に記述することが可能です。「識別情報」は全角 20 文字まで入力可能です。 ・CSV インポート機能を使用して、複数のパソコンに対して、異なるポリシーや識別情報を一括して適用することも可能です。詳細は「8.1 CSV インポート」を参照してください。

2．パソコン紛失時のデータ消去

万一パソコンを紛失した際は、以下の手順に沿ってパソコンに消去命令を発行します。管理サーバーからの命令を受信する必要があるため、対象となるパソコンを登録した時と同じ電話番号の SIM が挿入され、SMS を受信可能な状態であることが条件となります。データ消去が完了したパソコンはリモートロックされた状態になります。パソコンを再度ご利用になるには、ロック命令の解除が必要です。9 章 こんな時は の 9.1 データ消去が完了したパソコンを再利用する場合を参照ください。

※注意	・操作の対象となるパソコンが以下の状態の場合は、「消去命令」を受信することができません。 – 無線通信機能の電波を停止する設定になっている場合 – 通信エリア外またはエリア内の電波の届かない場所にある場合 – バッテリが切れている場合 – バッテリが取り外されている場合 – SMS が利用できるデータ通信契約を有する SIM カードが未挿入の場合 ・操作の対象となるパソコンが以下の状態の場合は、「消去命令」の受信または処理結果が応答できない可能性があります。 – 周囲で大量の通信が行われている、または回線の輻輳により良好な通信ができない場合 – 金属製の鞄に入れている場合など、通信が遮断され良好な通信ができない状態にある場合 – 通信エリア内であっても電波の届きにくい場所にある場合 – パソコンの動作保証条件に満たない環境の場合 – 電気通信事業者の通信網に障害が発生している場合 – APN が正しく設定されていない場合

STEP1 対象の確認

ID とパスワードで管理サーバーにログインし、HOME 画面で紛失したパソコンを PC 名や型名、電話番号等をもとに特定します。必要に応じて検索機能をご利用ください。

STEP2 消去命令を発行

対象となるパソコンの命令ボタンをクリックして[**消去**]をクリックします。確認画面が表示されたら[OK]をクリックします。

※注意	一度発行した「消去命令」は取り消す事ができません。

消去命令が発行されると、ステータスが**[消去発行中]**に変わり、命令ボタンがクリックできない状態になります。

該当のパソコンが SMS を受信すると、データ消去が発動します。消去が完了すると、管理サーバーに対して SMS で消去完了の通知が行われます。管理サーバーが消去完了通知を受信すると、ステータスが**[消去完了]**に変わります。あわせて、1章 STEP1 の⑩で指定した管理者のアドレス宛に通知メールが送信されます。

※注意	・結果返信には SMS での送信が行われます。この通信料金についてはお客さま負担となります。料金につきましてはお客さまのご契約を確認願います。

消去命令を受信した際のパソコンの挙動について

パソコンが電源オフまたは休止状態の場合、命令を受信すると自動的にパソコンの電源を投入して消去を実行します。パソコンが電源オン（Windows が起動中）の場合、命令を受信すると強制的に再起動を行ってから消去を実行します。パソコンがスリープ中の場合、命令を受信するとスリープから復帰したのち、強制的に再起動を行ってから消去を実行します。

消去命令の完了を確認できない場合

命令を発行してしばらくすると、ステータスが**[命令不達]**となり、命令の再発行が可能な状態となる場合があります。これは通信事業者側で、SMS（消去命令）の再送保持期間を過ぎた、あるいは何らかの事情により、通信事業者側で SMS の配送をあきらめた場合など、消去命令がパソコンに届かなかった事を表します。

また、命令発行から 3 時間が経過すると、ステータスが**[消去発行中]**のまま、命令の再発行が可能な状態となる場合があります。これは以下のいずれかの状態であることを表します。

- 管理サーバーから送信された SMS（消去命令）がパソコンに届かず、消去が実行されていない。ただし、通信事業者側で SMS を保持しており、自動的に再送が行われる可能性がある。
- 消去は完了したが、パソコンから送信された SMS（消去完了通知）が管理サーバーに届いていない。

これらの場合、命令ボタンが有効になり、再度命令を発行する事が可能となりますので、必要に応じて消去命令を再発行してください。

※注意	・暗号化機能付 HDD もしくは暗号化機能付フラッシュメモリディスク以外を搭載されている場合はデータ消去機能をご利用できません。 ・データ消去機能とは暗号化機能付 HDD/フラッシュメモリディスクにおいて、暗号化されたデータを復号するための暗号鍵を消去することにより、当該 HDD/フラッシュメモリディスクに保存されたデータを復元できなくするものです。 ・本サービスの「データ消去」機能は、HDD/フラッシュメモリディスク上の暗号化されたデータを消去するものではありません。 ・フラッシュメモリ(eMMC)搭載モデルについては全領域の上書き消去となります。 ・リモートによる消去を行う前に HDD／フラッシュメモリディスクが取り外された場合は、消去することはできません。

３．リモートロック・ロック解除

管理サーバーからの命令でロックやロック解除を実行します。ロックと同時にビープ（警告音）を鳴らすことも可能です。管理サーバーからの命令を受信する必要があるため、対象となるパソコンを登録した時と同じ電話番号の SIM が挿入され、SMS を受信可能な状態であることが条件となります。

※注意	・操作の対象となるパソコンが以下の状態の場合は、「ロック命令」「ビープ＆ロック」を受信することができません。 － 無線通信機能の電波を停止する設定になっている場合 － 通信エリア外またはエリア内の電波の届かない場所にある場合 － バッテリが切れている場合 － バッテリが取り外されている場合 － SMS が利用可能なデータ通信契約を有する SIM カードが未挿入の場合 ・操作の対象となるパソコンが以下の状態の場合は、「ロック命令」「ビープ＆ロック」の受信または処理結果が応答できない可能性があります。 － 周囲で大量の通信が行われている、または回線の輻輳により良好な通信ができない場合 － 金属製の鞄に入れている場合など、通信が遮断され良好な通信ができない状態にある場合 － 通信エリア内であっても電波の届きにくい場所にある場合 － パソコンの動作保証条件に満たない環境の場合 － 電気通信事業者の通信網に障害が発生している場合

ビープ機能について

ロック命令の発動時にパソコンにビープ（警告音）を鳴らして、紛失したパソコンの発見を促す機能です。ビープ機能を使用する場合、以下の手順で命令を発行する際に**[ビープ＆ロック]**を選択します。 [ビープ＆ロック]を選択した場合、ロックの発動とあわせて 1 分程度の間ビープ音が鳴ります。ロック中にパソコンの再起動を行った場合、起動時に再度ビープ音が鳴ります。

※注意	ビープ機能に対応していないパソコンでは[ビープ＆ロック]が選択できません。

STEP1 対象の確認

ID とパスワードで管理サーバーにログインし、HOME 画面でロックしたいパソコンをPC名や型名、電話番号等をもとに特定します。必要に応じて検索機能をご利用ください。

STEP2 ロック命令を発行

対象となるパソコンの命令ボタンをクリックして**[ロック]**または**[ビープ＆ロック]**をクリックします。確認画面が表示されたら[OK]をクリックします。

※注意	一度発行した「ロック命令」「ビープ＆ロック命令」は取り消す事ができません。

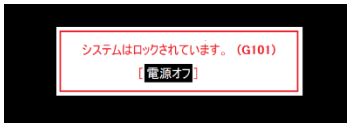
命令が発行されると、ステータスが**[ロック発行中]**または**[ビープ発行中]**に変わり、命令ボタンが押せない状態になります。

該当のパソコンが SMS を受信するとロックが発動します。ロックが完了すると、管理サーバーに対して SMS でロック完了の通知が行われます。管理サーバーがロック完了通知を受信すると、ステータスが**[ロック完了]**に変わります。[ビープ＆ロック]の場合はロックとあわせてビープ音が鳴ります。

※注意	・結果返信には SMS での送信が行われます。この通信料金についてはお客さま負担となります。料金につきましてはお客さまのご契約を確認願います。

ロック命令、ビープ＆ロック命令を受信した際のパソコンの挙動について

パソコンが電源オフまたは休止状態の場合、命令を受信すると自動的にパソコンの電源を投入してロックを実行します。
パソコンが電源オン（Windows が起動中）またはスリープ中の場合、命令を受信すると強制的に再起動を行ってからロックを実行します。
ロックが完了すると、以下の画面が表示されます。リターンキーを押すか、1 分程度経過するとシャットダウンします。



※注意	・パソコンが「ロック命令」「ビープ＆ロック命令」を受信した場合、対象となるパソコンの動作状況に関係なく再起動します。そのため命令を実行した際の状況によっては、以下の問題が起こる可能性があります。 - ロック解除後にパソコンが正しく起動しない - 作成中のデータが破壊される - HDD に保存されたデータが破壊される

STEP3 リモートロックの解除

リモートロックを解除するには、対象となるパソコンの命令ボタンをクリックして**[ロック解除]**をクリックします。確認画面が表示されたら**[OK]**をクリックします。

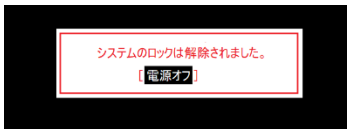
ロック解除命令が発行されると、ステータスが**[ロック解除発行中]**に変わり、命令ボタンが押せない状態になります。

該当のパソコンが SMS を受信するとロックが解除されます。ロックの解除が完了すると、管理サーバーに対して SMS でロック解除完了の通知が行われます。管理サーバーが解除完了通知を受信すると、ステータスが**[ロック解除完了]**に変わります。

※注意	ロック命令でロックされたパソコンは、後述の USB 解除キーでは解除できません。

ロック解除命令を受信した際のパソコンの挙動について

パソコンがロック中か、ロックされていない状態かにかかわらず、以下の挙動となります。
パソコンが電源オフまたは休止状態の場合、命令を受信すると自動的にパソコンの電源を投入してロックを解除します。パソコンが電源オン（Windows が起動中）またはスリープ中の場合、命令を受信すると強制的に再起動を行ってからロックを解除します。ロック解除が完了すると、以下の画面が表示されます。リターンキーを押すか、1 分程度経過するとシャットダウンします。



※注意	・対象のパソコンが「ロック解除命令」を受信した場合、パソコンの動作状況に関係なく再起動します。そのため命令を実行した際の状況によっては、以下の問題が起こる可能性があります。 - ロック解除後にパソコンが正しく起動しない - 作成中のデータが破壊される - HDD に保存されたデータが破壊される

ロック命令、ビープ＆ロック命令、ロック解除命令の完了を確認できない場合

命令を発行してしばらくすると、ステータスが**[命令不達]**となり、命令の再発行が可能な状態となる場合があります。これは通信事業者側で、SMS（命令）の再送保持期間を過ぎた、あるいは何らかの事情により、通信事業者側で SMS の配送をあきらめた場合など、命令がパソコンに届かなかった事を表します。

また命令発行から 3 時間が経過すると、ステータスが**[xxx発行中]** のまま、命令の再発行が可能な状態となる場合があります。これは以下のいずれかの状態であることを表します。

- 管理サーバーから送信された SMS（命令）がパソコンに届かず、ロックやロック解除が実行されていない。ただし、通信事業者側で SMS を保持しており、自動的に再送が行われる可能性がある。
- ロックやロック解除は完了したが、パソコンから送信された SMS（完了通知）が管理サーバーに届いていない。

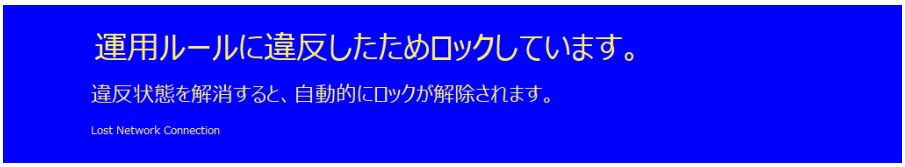
これらの場合、命令ボタンが有効になり、再度命令を発行する事が可能となりますので、必要に応じて命令を再発行してください。

４．ポリシー監視ロック

パソコンが適用している監視ポリシーに違反する挙動を検知すると操作ロックを発動します。パソコンが管理サーバーと通信できない状態であっても、あらかじめ指定したポリシーを監視し、自律的に操作ロックを発動する事が可能なため、不正利用の防止や不正持ち出しの防止に効果的です。

ポリシー監視ロックが発動した際のパソコンの挙動について

パソコンが電源オフ、休止状態、またはスリープ中の場合、ポリシー監視ロックは発動しません。
パソコンが電源オン（Windows が起動中）の場合、ポリシー違反を検知すると操作ロックを実行します。
操作ロックが行われると、マウス、キーボード、タッチパネル等の入力デバイスを無効化されパソコンが操作不能になり、１章 STEP2 ⑫で指定したメッセージが表示されます。操作ロック発動中は再起動を行っても操作不能な状態が継続します。



※注意	・リモートロックとポリシー監視ロック（操作ロック）では、ロックの方式、表示される画面、解除方法が異なります。 ・ご利用の環境によっては、操作ロックの実行中にロック画面が表示されずに黒い画面や Windows にログオンする前の画面などが表示されることがあります。ロック画面が表示されない場合でも操作ロックの発動中は入力デバイスが無効化されているため、パソコンの操作は不可能です。

ポリシー監視ロックの解除

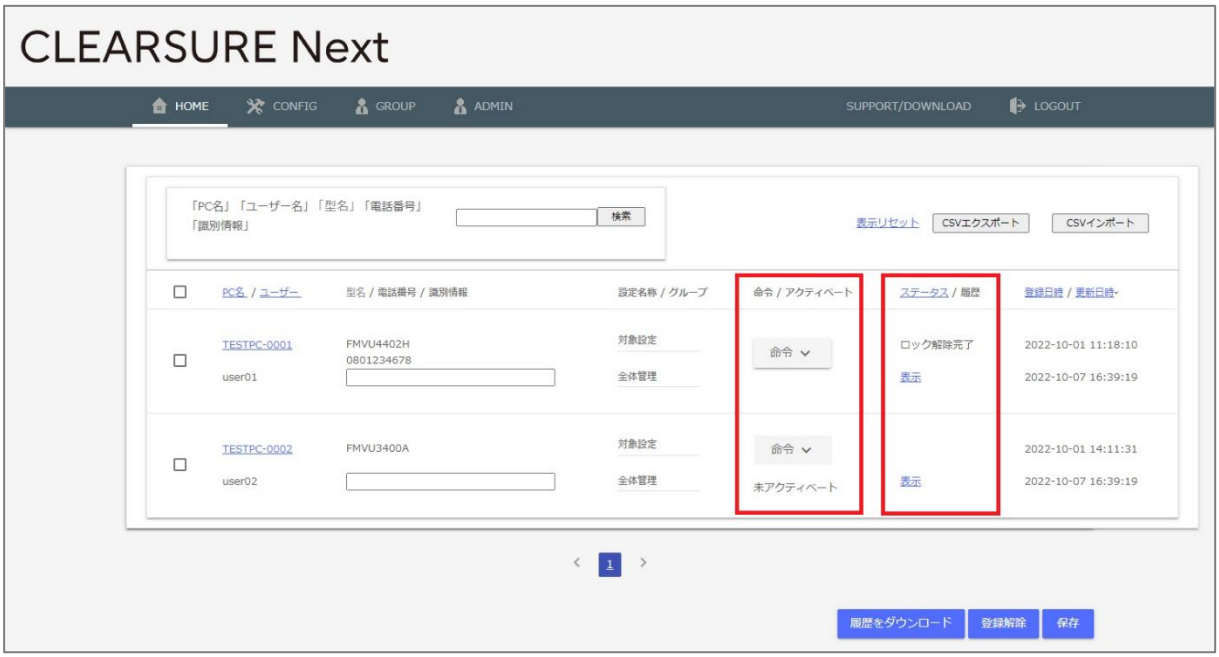
ポリシー監視ロックが発動した場合の解除方法は次の2つの方法があります。

■ポリシーの条件を満たすことによるロック解除
ロック実行後に、パソコンがポリシーを満たす状態に戻ると自動でロックを解除します。
（例；オフライン監視を ON にしている場合、オフラインになるとロックしますが、オンラインになるとロックが解除されます）
■USB 解除キーによるロック解除
CONFIG 画面でロック解除キーファイル（Unlock.txt）をダウンロードし、市販の USB メモリまたは SD カードのルートフォルダに保存します。操作ロック発動中に USB キーをパソコンに挿すことでロックを解除することができます。ロック解除キーは、あらかじめ CONFIG 画面で 4 文字以上 32 文字以内の半角英数字を指定しておく必要があります。詳細は「1. 基本セットアップ STEP2」を参照してください。

※注意	・USB ポートまたは SD カードスロットがないタブレット等ではこのアンロック方法はご利用できません。監視対象のパソコンの USB ポートが利用可能か確認してください。 ・同じ監視ポリシーを持つパソコンはすべて同一の解除キーが適用されます。 キーファイルのファイル名は絶対に変更しないでください。 ・管理サーバーで解除キーを更新してもパソコンが管理サーバーにアクセスするまではパソコン側の解除キーは以前のままです。古い解除キーがなければロックを解除できません。キーを更新する前に現行のキーを保存しおいてください。 ・USB 解除キーを使用する場合、Windows 起動後に USB を挿してください。

５．データ消去やリモートロックの進捗を確認するには

管理サーバーの HOME 画面で各パソコンの状況を確認できます。



5.1 アクティベート状態とステータス

パソコンの登録状態、および命令の通達状態を表示します。

アクティベート状態	命令の発行可否	クライアントの状態
空白	命令の発行が可能	正常な状態
非対応	命令の発行は不可	CLEARSURE の対象機種ではない または必要な条件を満たしていない
SIM なし	命令の発行は不可	SIM が挿入されていない、または認識できない
未アクティベート	命令の発行は不可	BIOS 機能が有効化されていない

ステータス表示	命令の通達状況	クライアントの状態
消去発行中	消去命令を発行した後、応答が未着	不明
消去完了	消去命令の実行完了を確認	消去完了
ロック発行中 ビープ発行中	ロック命令を発行した後、応答が未着 ビープ＆ロック命令を発行した後、応答が未着	不明
ロック完了	ロック命令／ロック&ビープ命令の実行完了を確認	ロック完了
ロック解除発行中	ロック解除命令を発行した後、応答が未着	不明
ロック解除完了	ロック解除命令の実行完了を確認	ロック解除完了
命令不達	命令がパソコンに届かず、通信事業者側での再配送も行われない	不明
命令受信済	通信事業者側での命令配送は完了した（命令がパソコンに届いたと見込まれる）が、応答が未着	不明

※注意	・ポリシー監視によるパソコンのロック／ロック解除などの状態は履歴画面にのみ表示され、ステータスには表示されません。

5.2 履歴

[履歴]欄の**[表示]**リンクをクリックすると、該当のパソコンの履歴画面が表示されます。履歴画面ではポリシー違反の発生状況およびデータ消去命令やリモートロック命令の実行状況を確認できます。ポリシー違反の履歴はパソコンが管理サーバーと通信するタイミングで受信するため、リアルタイムでの表示ではありません。
また、後述する「データ適正消去実行証明書」もこの画面から発行します。「データ適正消去実行証明書」については、7 項を参照してください。

① 発動日時
ポリシー違反の発生日時、またはリモート命令の実行日時を表示します。
リモート命令の履歴に関しては、管理サーバーから命令を発行した日時、および管理サーバーが実行完了通知を受信した日時を表示します。

② アクション
ロック、ロック解除、消去など、実行したアクションを表示します。

③ 発動理由
検出した違反の種類を表示します。

④ 端末情報
命令実行時、および違反検出時に位置測定に成功した場合、パソコンの位置情報を表示します。
また、命令実行時のバッテリー残量と最終起動日時を表示します。

※ヒント	・パソコンの盗難や紛失が発生した際、リモート命令の実行完了履歴の「端末情報」に表示される「最終起動日時」が、事故発生の前か後かを確認することで、事故発生後の不正操作の有無を推測することが可能です。 ・最終起動日時は端末の電源を入れた後、「FUJITSU」ロゴが表示されたタイミングで記録されます。BIOS パスワードを設定している場合は、正しい BIOS パスワードが入力された時点で記録されます。

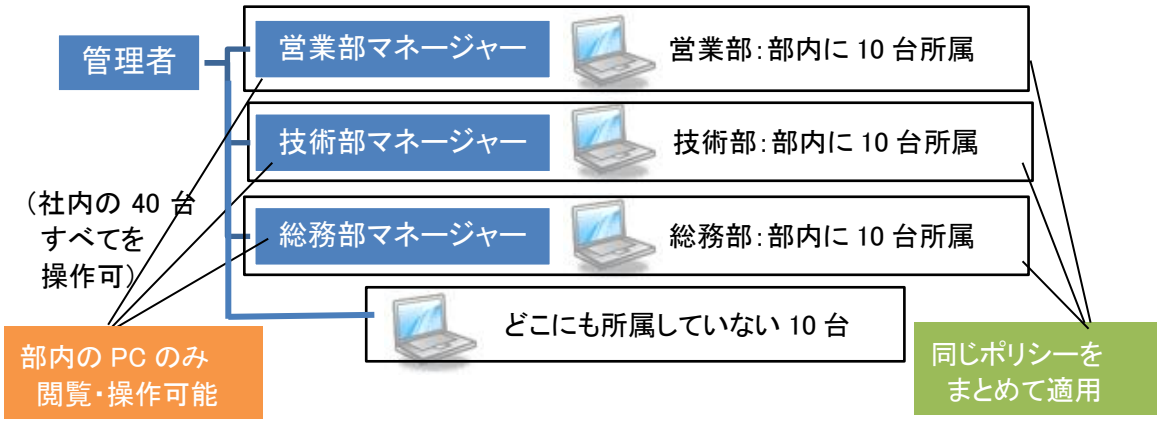
⑤ ログイン ID
命令を発行した管理者の ID を表示します。

⑥ 証明書
データ適正消去実行証明書の[発行申請]、[表示]ボタンを表示します。

※注意	・リモート命令実行時はひとつの命令につき、命令を発行した管理サーバー側の履歴とパソコンから受信した実行完了履歴の 2 つの履歴が表示されます。 ・位置情報は、パソコン内蔵の GPS を利用し、パソコンが、命令を実行したタイミング、または違反を検出したタイミングで、BIOS または Windows の機能を利用して測定し記録します。GPS の電波が受信できない場合、位置情報は取得できないため、履歴上に表示されません。

6. グループ管理機能

企業(または組織)内で複数のパソコンを使用している場合、各部署の業務内容に応じて運用ルールやパソコン内に保存されたデータの重要性が異なります。グループ管理機能は、社内のパソコンを所属部署別に分類し、部署(グループ)ごとに異なるポリシー(設定)を適用する場合や、各部署の責任者による個別管理を行うための機能です。



※ヒント	組織内のすべてのパソコンを管理者が一元管理する場合には、本機能の設定は必要ありません。

6.1 管理者権限とユーザー権限 (グループ責任者)

管理者

- ◆ 管理サーバーのすべての機能を操作できます。
- ◆ 対象設定の作成・変更、データ消去命令・ロック命令・ロック解除命令の発行、履歴の閲覧・削除等を実行することができます。
- ◆ グループを作成し、任意のパソコンの所属グループを選択または移動することができます。
- ◆ 管理者やグループ責任者の追加、削除、および所属グループやパスワードを変更することができます。

ユーザー(グループ責任者)

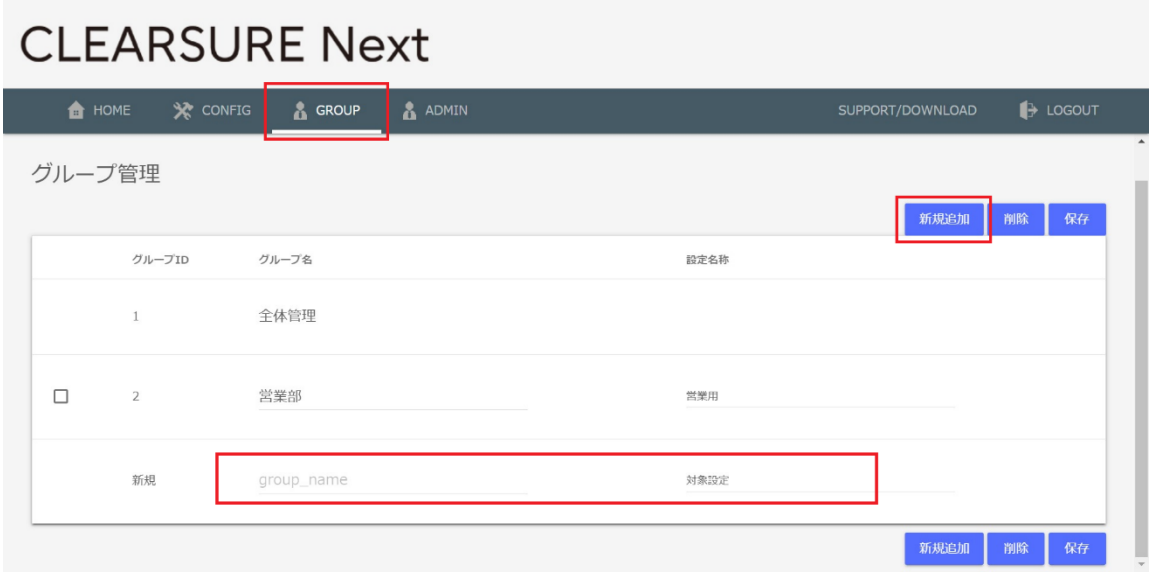
- ◆ グループ責任者は自分が担当するグループに属するパソコンに対して、データ消去命令・ロック命令・ロック解除命令の発行、および PC 情報の確認、履歴の閲覧を実行できます。

ユーザー権限の制限事項

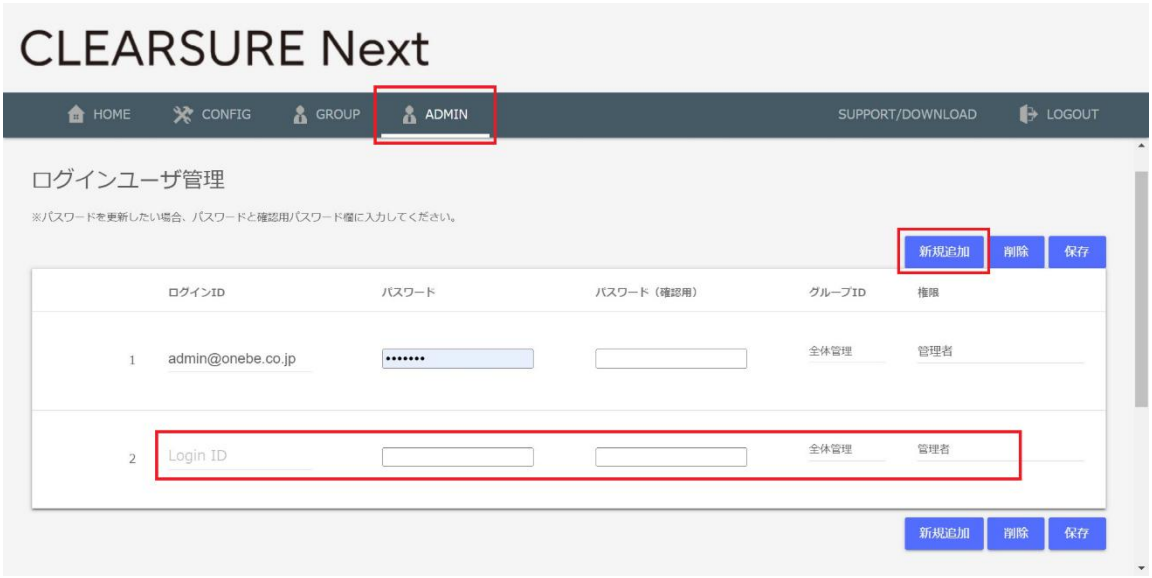
- ◆ GROUP 画面、ADMIN 画面は利用できません。
- ◆ CONFIG 画面は閲覧のみ可能です。
- ◆ 所属グループが異なるパソコンの操作や閲覧はできません。
- ◆ 登録されているパソコンの所属グループや設定の変更はできません。
- ◆ 登録されているパソコンの登録解除、履歴の削除はできません。

6.2 グループの作成

グループ管理機能を利用するにはまずグループの登録が必要です。この作業は管理者のみ操作可能です。GROUP 画面で**[新規追加]**ボタンをクリックし、作成されたレコードの**[グループ名]**を記入し、グループに適用する設定を**[設定名称]**で選択します。必要な情報を入力したら、画面右側の**[保存]**ボタンをクリックします。



続いて ADMIN 画面で[新規追加]ボタンをクリックし、作成されたレコードの**[ログイン ID]**と**[パスワード]**を記入し、**[グループ ID]**で管理対象のグループを、**[権限]**で管理者かグループ責任者（ユーザー）を選択します。必要な情報を入力したら、画面右側の**[保存]**ボタンをクリックしてください。

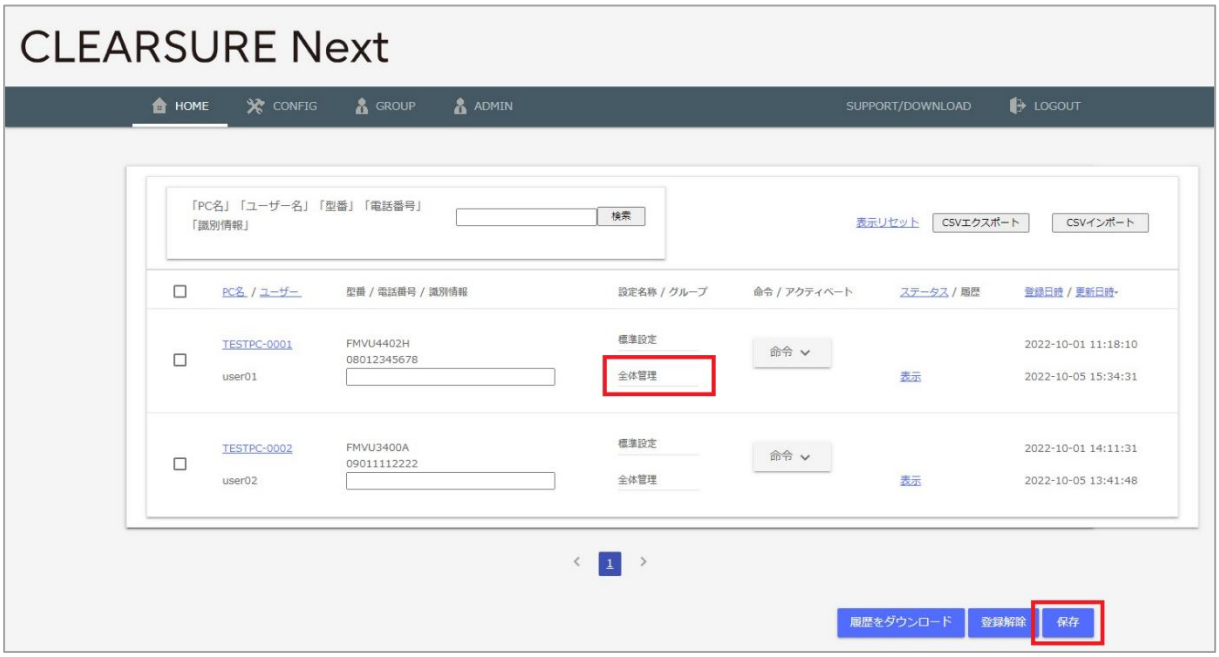


※注意	・ログイン中の管理者、登録済みのパソコンに適用中のグループは削除できません。 ・各項目を変更した場合は必ず[保存]ボタンをクリックしてください。
※ヒント	・グループ ID を「全体管理」、権限を「ユーザー」と指定することで、組織内のすべてのパソコンを対象としたグループ責任者（ユーザー）を作成することも可能です。 ・ログイン ID は 4～32 文字の半角英数字および記号になります。メールアドレスを使用して頂くことを推奨します。 ・パスワードは、4～32 文字の半角英数字、および記号になります。 ・グループは 50 個まで作成できます。 ・管理者、グループ責任者(ユーザー)は合計で 50 個まで作成できます。

6.3 所属グループの指定

グループ登録が完了したら続いてパソコンの所属先のグループを指定します。この作業も管理者のみ操作可能です。

HOME 画面で対象パソコンの**[グループ]**で、プルダウンから任意のグループ名を選択します。画面内で必要なパソコンのグループ選択がすべて完了したら、画面右下の**[保存]**ボタンをクリックします。保存が完了すると、グループで指定された設定が反映さます。



※注意	・所属グループや対象設定を変更した場合は、必ず[保存]ボタンをクリックしてください。多くのパソコンを管理し、HOME 画面が複数ページにわかれる場合は、他のページに移動する前に[保存]する必要があります。 ・グループや設定を変更してもパソコンが管理サーバーと通信するまでは、以前の設定で監視を続けます。管理サーバーと通信すると新しい設定が反映されます。
※ヒント	・グループに所属しているパソコンに、個別の設定を適用することはできません。個別の設定を適用する必要がある場合には、「全体管理」を指定してください。 ・CSV インポート機能を使用して、複数のパソコンに対してグループを一括して指定することも可能です。詳細は「8.1 CSV インポート」を参照してください。

7． データ適正消去実行証明書

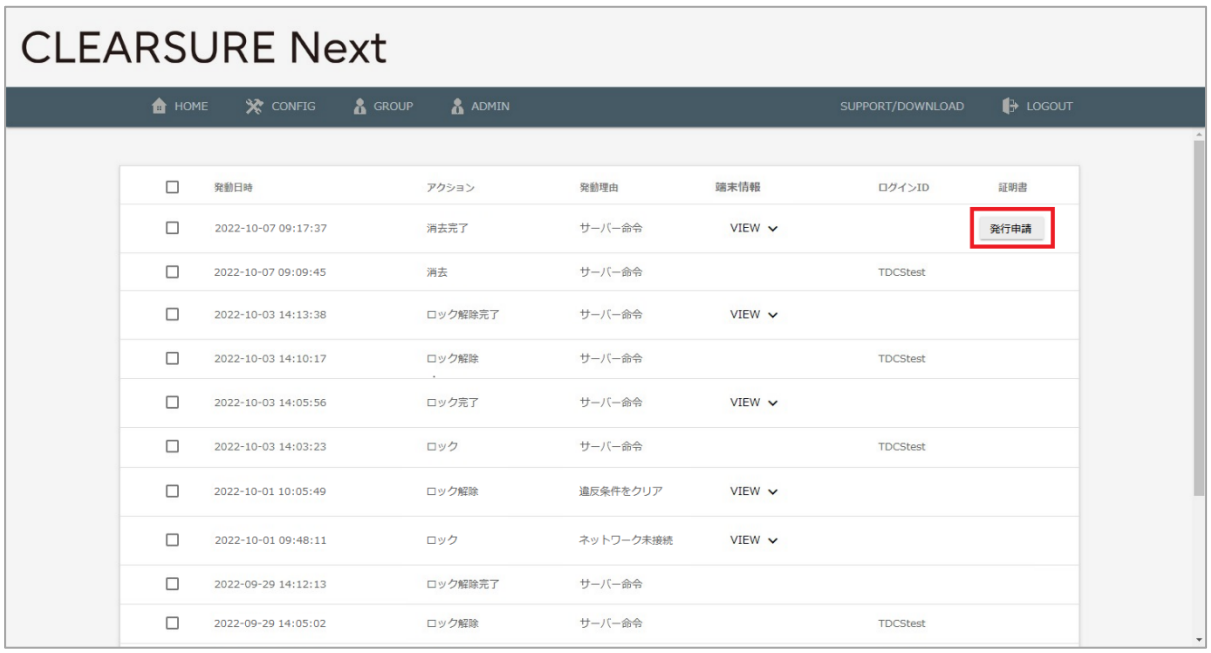
盗難や紛失などの事故が発生した際、あるいはパソコンの廃棄やリースアップの際などに、ドライブ上の全データを消去したうえで、データ適正消去実行証明協議会(略称 ADEC) が発行する「データ適正消去実行証明書」を取得、閲覧することが可能です。「データ適正消去実行証明書」には、消去を実施したパソコンおよびドライブの情報のほか、消去に使用したソフトウェアの情報、消去を実行した日時と実行結果などが記載されており、記載内容による適正な消去が実行されたことが、ADEC によって証明されます。

7.1 証明書発行条件

・証明書発行可能枚数（1章STEP1 ⑦参照）が 1 以上である事
・データ消去命令を発行し、消去完了通知を受信済みの状態である事（詳細は2章を参照）
・フラッシュメモリ(eMMC)搭載モデルではない事

7.2 証明書の発行

HOME 画面から対象とするパソコンの「履歴」をクリックし、**[発行申請]**ボタンをクリックします。しばらくすると、ボタンが**[表示]**に変わります。**[表示]**ボタンをクリックすると、「データ適正消去実行証明書」が表示されます。



※注意	・パソコン側でデータ消去が完了している場合でも、管理サーバーに消去完了の通知が届かない場合や消去対象のドライブが存在しない場合は、データ適正消去証明書を発行することはできません。 ・データ適正消去実行証明書に記載される「完了日時」および「消去終了日時」は、履歴メニューの「発動日時」と異なります。 ・登録解除（8.4 項）を行うと、データ適正消去実行証明書の発行・閲覧ができなくなります。廃棄消去が完了したパソコンのデータ適正消去実行証明書は、登録解除を行う前に発行・ダウンロードを行い、適切な方法で保管してください。 ・CLEARSURE Next の契約更新月をこえると、証明書の発行可能枚数がリセットされます。契約を更新される場合も、発行可能枚数の残存分が翌年に繰り越される事はありません。

（証明書サンプル）

2024年04月23日
発行 ID000000002871

データ適正消去実行証明書

データ適正消去実行証明協議会 {略称：ADEC(Association of Data Erase Certification)} は、本協議会が認証したデータ消去ソフトウェアおよび消去事業者により実施された消去の結果を下記の通り証明します。

消去パソコン情報

メーカー名 / 型番	FUJITSU/FMVU4402H
製造番号（シリアル）	R2804110
ドライブ情報 （モデル名/製造番号/容量）	Micron_MTFDKBA256TFK-1BC15ABFA / 22263901EF22

消去情報

消去事業者情報	事業者 ID	： 0001	
	事業者名	： TESTワンビ株式会社 TEST本社	
	レーティング	：	
消去ソフトウェア情報	メーカー名	： 富士通クライアントコンピューティング	
	ソフトウェア名	： Erase Disk	
	認証番号	： ADEC-S2020-005	
	消去方法	： PC対応（SSD:SATA,NVMe）	
消去実行日時	開始：2024/04/23 15:23:59		終了：2024/04/23 15:23:59
消去結果	○		

証明書発行シリアルナンバー ： TDCS_test_249697

一般社団法人 ソフトウェア協会について
ソフトウェア製品に係わる企業が集まり、ソフトウェア産業の発展に係わる事業を通じて、我が国産業の健全な発展と国民生活の向上に寄与することを目的としている一般社団法人です。

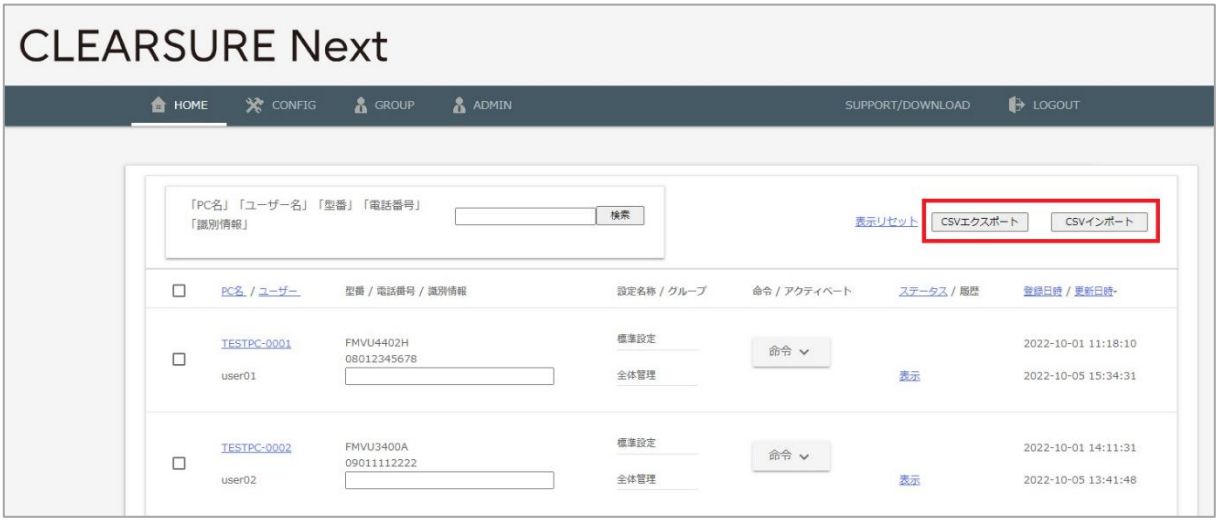
データ適正消去実行証明協議会について
データの適正な消去のあり方を調査・研究し、その技術的な基準の策定とデータが適正に消去されたことを第三者機関が証明する制度の普及・啓発を推進する協議会です。

ADEC
データ適正消去実行証明協議会

8．その他の機能

8.1 CSV インポート

「HOME」画面から CSV ファイルを使用してパソコン一覧情報の取得、グループやポリシーの一括変更が可能です。「CSV エクスポート」ボタンをクリックすると、登録パソコン情報の一覧を CSV 形式でダウンロードします。ダウンロードしたファイルを編集し、「CSV インポート」ボタンで取り込むことで、一部の項目の値を更新します。



[CSV ファイルの変更可能な項目について]
CSV インポート時に変更可能な項目は下記の3項目です。下記以外の項目は変更しないでください。
・設定 NO:「CONFIG」画面に表示される「No.」です。指定したい設定の番号（設定名称ではありません）を1～10の数値（半角数字）で指定してください。
・グループ ID:「GROUP」画面に表示される「グループ ID」です。指定したいグループの ID を1～10の数値（半角数字）で指定してください。
・識別情報:「HOME」画面に表示される「識別情報」です。パソコンや利用者を特定するための情報を全角 20 文字以下で指定してください。

※注意	・CSV データの先頭行に表示された各項目名や列の順序を変更しないでください。また、先頭行は削除しないでください。 ・「設定 NO」（2 列目）と「グループ ID」（3 列目）「識別情報」（4 列目）以外の項目は変更しないでください。その他の項目を変更してインポートを行っても設定には反映されず、エラーとなる場合があります。また「端末 ID」を変更すると、意図しないパソコンの設定が変更される場合があります。 ・エクスポートした CSV を Microsoft Excel などの表計算ソフトで変更・保存すると、値が加工されてインポート時にエラーになる場合があります。インポートを行う場合には、テキストエディタでの編集をおすすめします。
※ヒント	・一部のパソコンのみのインポートが可能です。インポートしたデータに含まれていないパソコンの設定は変更されません。 ・CSV インポートを使用して、パソコンの登録解除を行うことはできません。 ・「グループ ID」で「1」（全体管理）以外のグループを指定した場合、「設定 NO」の指定に関わらず、「グループ管理」で指定された設定が適用されます。 パソコンごとに異なる設定を適用したい場合には、対象となるパソコンの「グループ ID」に「1」を指定してください。

8.2 PC 情報

登録された管理対象のパソコンのハードウェア情報や OS 情報、ネットワーク情報などを表示します。表示内容は24時間で自動的に更新されます。ただし、対象のパソコンがネットワークに接続されていない場合、情報は更新されません。

① 履歴
管理対象のパソコンの、命令発行および命令実行の履歴を表示します。表示内容については 5.2 項を参照してください。

表示される項目

◆ ソフトウェア情報
更新日時（最後に管理サーバーとの通信が行われた日時）、ログインユーザー名、クライアントプログラムのバージョン、製品シリアル番号、契約終了日、OS 種類、OS バージョン、最終起動日時、UEFI 起動状態、CLEARSURE アクティベート状態

◆ PC 情報
PC 名、型名、メーカー、製造番号、BIOS 情報、CPU 情報、メモリサイズ、ドライブ名、ファイルシステム、ドライブサイズ、空き領域、物理ドライブ型番、物理ドライブ容量、物理ドライブシリアル番号

◆ 携帯ネットワーク情報
携帯電話番号、型番、ファームウェア、ICCID

◆ ネットワークハード情報
アダプター名、MAC アドレス

◆ ネットワーク接続情報
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、DHCP 設定状態

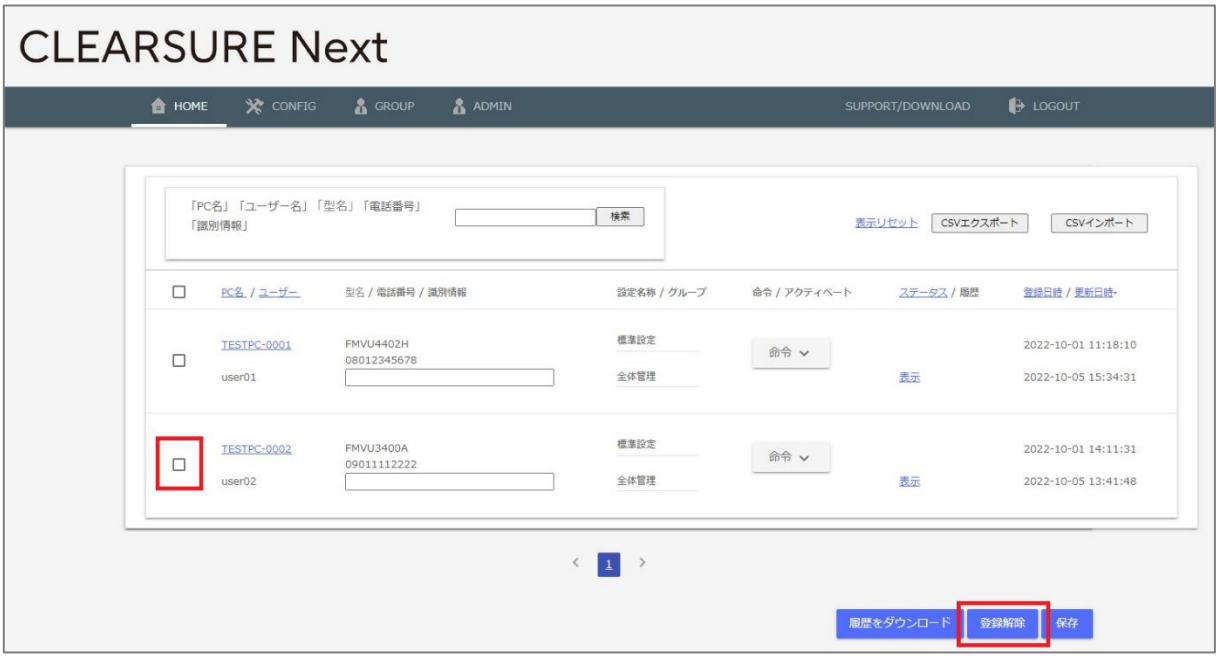
8.3 パソコンの登録解除

次のような場合は登録済みのパソコンの登録解除を行う（管理対象から外す）必要があります。

◆ 新しいパソコンに買い換え、古いパソコンの利用を停止する場合
◆ OS の再セットアップなどでクライアントプログラムを再インストールする場合
◆ 契約台数が不足し、一部のパソコンを管理から除外する場合

登録解除の手順

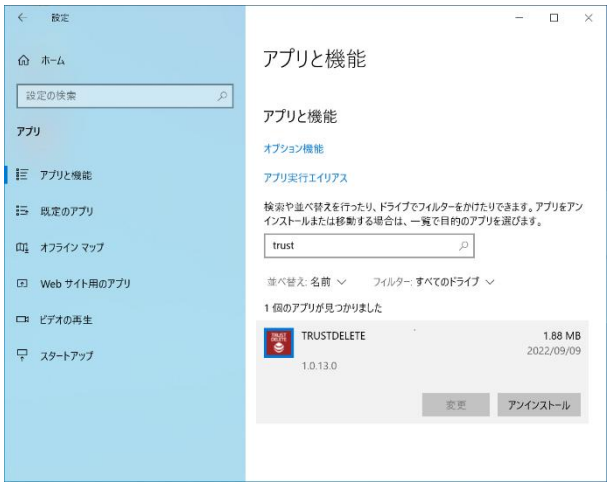
HOME 画面で登録解除を行うパソコンの左端のボックスにチェックを入れてから画面下の**[登録解除]**ボタンをクリックします。登録解除の確認画面が表示されたら OK をクリックします。以上でこのパソコンの登録が削除され 1 台分の空きができます。



※注意	・登録解除ボタンをクリックする前に左端のボックスに必ずチェックを入れてください。 ・管理サーバー側で登録解除を完了した後で、管理サーバーとの通信を行ったパソコンは、CLEARSURE Next の全機能が停止します。 ・パソコンを紛失した際には、「消去命令」または「ロック命令」を発行し、命令の実行が確認できるまで、対象パソコンの登録解除は実施しない事を推奨いたします。 ・登録解除を行ったパソコンの履歴情報およびデータ適正消去実行証明書は管理サーバーから確認できなくなります。登録解除を実施する前に「7.2 証明書の発行」などにより、必要な情報を保存してください。

8.4 クライアントプログラムのアンインストール

管理対象パソコンから CLEARSURE Next のクライアントプログラムをアンインストールする際は、対象パソコンで[設定]の[アプリと機能]（またはコントロールパネルの[プログラムのアンインストールまたは変更]）を選択し、TRUST DELETE の**[アンインストール]**をクリックします。

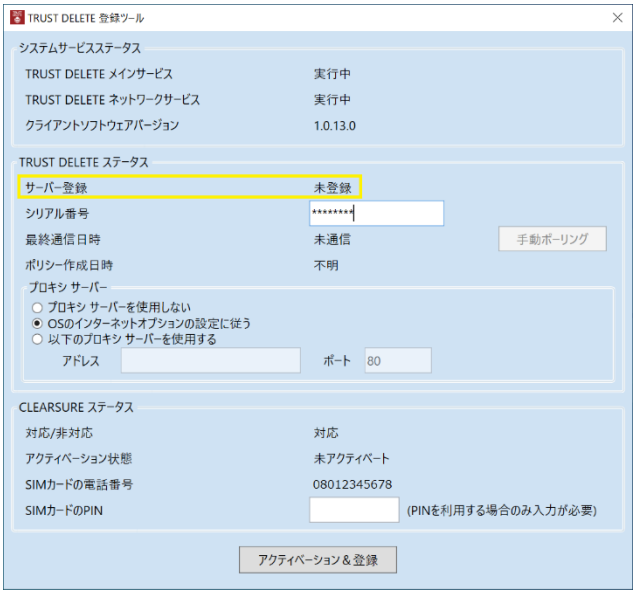


ウィザードに従ってアンインストールを実施してください。アンインストールパスワードをたずねられたら管理サーバーの CONFIG 画面で指定されたアンインストールパスワード（1章 STEP2 ②参照）を入力してください。

アンインストールが完了したら、再起動が必要です。

管理サーバー側で登録解除を完了した後で、管理サーバーとの通信を行ったパソコンでは、TRUST DELETE 登録ツールに表示される登録ステータスが「未登録」状態に戻ります。

この場合、アンインストールパスワードを入力することなく、アンインストールを行うことが可能です。



8.5 クライアントプログラムの更新（上書きインストール）

1. 管理サーバーにログインして上部のメニューから SUPPORT/DOWNLOAD 画面を開きます。

2. 別ウインドウでサポートページが開いたら、CLEARSURE Next プログラムのダウンロードの[こちらからダウンロード]をクリックして最新のプログラムを管理対象のパソコンに保存します。

3. 管理対象のパソコン上で、取得したプログラム（TDCSInst.exe）をダブルクリックし、旧バージョンからの更新（アップグレード）を確認するメッセージが表示されたら OK をクリックします。

4. そのままウィザードに従ってインストールし、インストールが完了したら再起動を行ってください。以上でクライアントプログラムの更新作業は終了です。

９． こんな時は

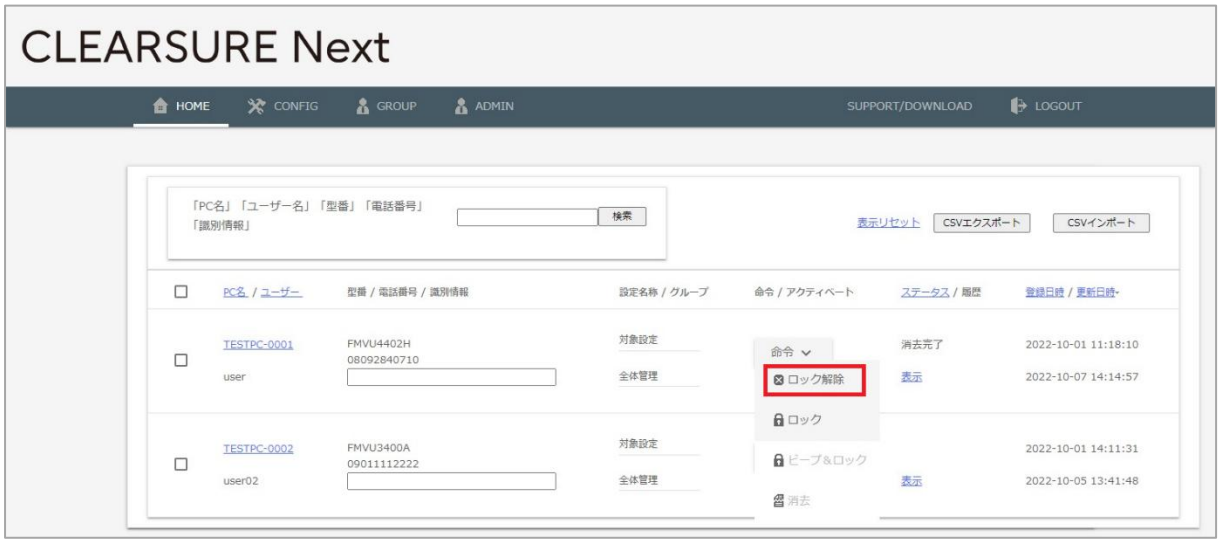
9.1 データ消去が完了したパソコンを再利用する場合

データ消去が完了したパソコンは、暗号化 HDD/フラッシュメモリディスクが消去された状態となります。また、同時にリモートロックが完了した状態となるため、そのままの状態ではリカバリーなどを実施することもできません。

データ消去が完了したパソコンが手元に戻った場合や、リース返却あるいは検証など目的で消去を実施した場合など、該当のパソコンを再度利用可能な状態にする場合には、以下の手順を実施してください。

※注意	・本手順を実施する前にデータ消去が完了したパソコンの登録解除を実施した場合、パソコンの再利用を行う事ができず、メーカー修理が必要となる場合があります。再利用する可能性のあるパソコンは、本手順が完了するまで登録解除を行わないでください。

1. HOME 画面から該当のパソコンの「ロック解除」を実行します。（詳細は 3 章 STEP3を参照）



※注意	・消去が完了したパソコンに対しては、ロック＆ビープ命令、消去命令を発行する事はできません。また、消去が完了したパソコンに対して、ロック解除を実行すると、それ以降すべての命令が発行できなくなります。 ロックが解除されたパソコンは再利用が可能な状態となりますので、消去が完了したパソコンに対してロック解除を行う場合には、該当のパソコンが手元にある状態で実行してください。

2. リカバリディスクなどを使用し、パソコンの再セットアップを実施します。リカバリーの手順については、パソコン本体に添付のマニュアルなどを参照してください。

3. 再セットアップが完了したら、1 章 STEP3 手順 1～4 に従ってクライアントプログラムのインストールを実施してください。

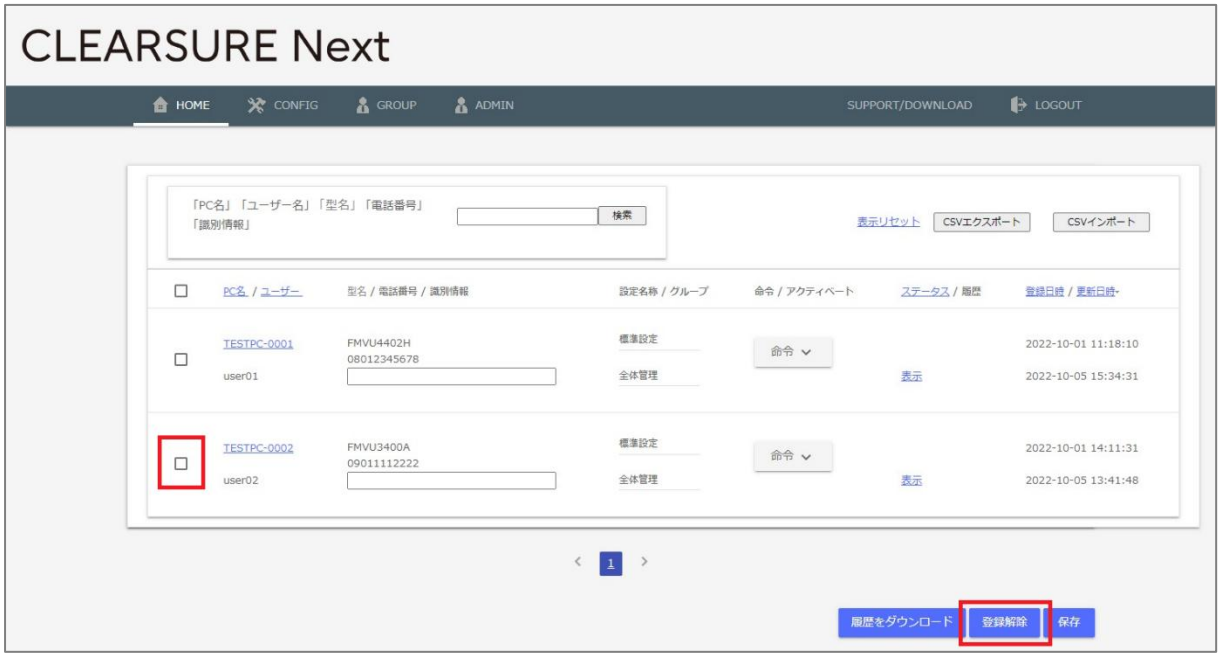
4. パソコンを引き続き CLEARSURE Next で管理する場合には、1 章 STEP3 手順 5 以降を実施し、アクティベーションと登録処理を実施してください。

5. パソコンをリース会社に返却する場合や他の用途に転用する場合など、CLEARSURE Next による管理を停止する場合には、8.3 項に従って該当のパソコンの登録解除を実施したあと、8.4 項に従ってクライアントプログラムのアンインストールを実施してください。

9.2 運用中に SIM を変更する／SIM の利用を開始する場合

登録済みのパソコンで、利用中の SIM を変更する場合、あるいは新たに SIM の利用を開始する場合、該当のパソコンの再登録が必要となります。以下の手順に従って再登録を実施してください。

1. HOME 画面から該当のパソコンの登録解除を実施します。（詳細は 8.3 項を参照）



2. パソコンをシャットダウンし、SIM の差替え（または挿入）を行ってから電源を投入します。

3. パソコンが起動したら「TRUST DLETE」を実行します。（詳細は 1 章 STEP3 を参照）

4. 「TRUST DELETE 登録ツール」が起動したら、サーバー登録が「未登録」となっていること、SIM カードの電話番号が正しく表示されていることを確認して**[アクティベーション＆登録]**ボタンをクリックします。
サーバー登録が「登録済み」になっている場合は、**[手動ポーリング]**をクリックしたあと、手順 3 からやりなおしてください。

5. 「登録とアクティベーションが完了しました。CLEARSURE の機能を利用するには再起動が必要です。」と表示されたらパソコンを再起動してください。

以上でクライアントの利用準備は完了です。

※注意	・アクティベーション完了後は必ずパソコンを再起動してください。 ・登録を完了しなければ本プログラムは正しく動作しません。必ず登録を行ってください。

9.3 パソコンの修理を行う場合

パソコンを修理に出す場合は、事前に CLEARSURE Next のクライアントプログラムのアンインストールを実施してください。パソコンが起動できない状態など、修理に出す前にアンインストールができない状態の場合は、修理完了後にクライアントプログラムのアンインストールを実施してください。
この際、管理サーバー側での「登録解除」を実施する必要はありませんが、アンインストールパスワードを入力させたくない場合などは、「登録解除」を実施しても差し支えありません。
登録解除の手順は 8.3 項を、アンインストールの手順は 8.4 項をご参照ください。

修理内容によっては、クライアントプログラムの再インストールは必須ではない場合もありますが、マザーボードや通信モジュール、HDD などのハードウェア交換を伴う修理の場合には、クライアントプログラムの再インストールと登録およびアクティベーションを必ず実施する必要があります。

修理完了後、利用を再開するためには、1 章 STEP3 に従ってクライアントプログラムのインストールと登録処理を実施してください。

※注意	マザーボードなどの交換を伴う修理後に利用再開の処理を実施した際、管理サーバーの HOME 画面上に修理前のパソコンと、修理後のパソコンが双方表示される場合があります。この場合、「登録日時」や「更新日時」を参照の上、修理前のパソコンの「登録解除」を実施してください。

9.4 「未アクティベーション」と表示され、命令発行できない場合

HOME画面の[アクティベート]欄に「未アクティベーション」と表示され、命令ボタンが押せない状態となっている場合、以下のいずれかの状態であることが推測されます。

- アクティベーション＆登録処理を実施した後、再起動が行われていない。
  この場合、該当のパソコンの再起動を実施してください。再起動後、管理サーバーとの通信が行われることで命令を発行可能な状態に移行します。
  該当のパソコンで「高速スタートアップ」機能が有効になっている場合など、電源 OFF/ON では正しい処理が行われない場合がありますので、必ず再起動を実施してください。

- 製品を利用するための要件が満たされていない。
  データ消去機能、リモートロック機能、ビープ機能を利用するために必要な、ドライバやファームウェアがインストールされていない可能性があります。1 章 STEP3 の手順1を参照の上、必要なドライバやファームウェアのインストール、更新作業を実施してください。
  必要なドライバ、ファームウェアの適用が完了しているにもかかわらず状況が改善しない場合や、インストールに失敗する場合などは、ハードウェアのサポート窓口または販売店にご相談ください。