遠隔データ消去サービス prime

管理サーバーマニュアル

- Ver.2.1-

はじめに

このたびは、遠隔データ消去サービス prime をご利用いただき、ありがとうございます。本サービスは、盗難・紛失時にコンピューター内のデータを消去するためのセキュリティサービスです。近年多発しているコンピューターの盗難・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、不正持出しの防止、不正利用の防止にも効果的です。

このマニュアルは、遠隔データ消去サービス prime の管理サーバーの設定方法および操作方法について説明しています。

■コンピューターを紛失した場合、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。

- ✓ **紛失時にどのコンピューター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://datawipeprm.nec-lavie.jp/admin/logindwp**
- ✓ **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。

TDP2040528

目次

遠隔データ消去サービス prime とは

■サービス概要

本サービスは、コンピューターの不正利用や盗難・紛失対策のためのセキュリティソリューションです。管理サーバーで設定した監視ポリシーに基づいてコンピューター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コンピューターをロックや強制シャットダウンします。複数の監視項目を組み合わせることでコンピューターのご利用場所やご利用目的に応じたポリシーを設定することが可能です。さらに管理サーバーからネットワークを経由して遠隔でコンピューターのロックや消去が可能です。

■主な機能

◆ データ消去

コンピューターの盗難・紛失時や廃棄時に OS を含むドライブ上の全データを消去する機能です。データ消去には3通りの実行方法があります。

消去命令： 管理サーバーから消去命令を発行します。対象となるコンピューターがネットワークで管理サーバーと通信できることが必要です。

自動消去： 一定時間コンピューターがネットワークに接続しない状態が継続した場合、時限稼働で消去を実行します。ネットワークにつながる可能性の低い紛失コンピューターなど、消去命令を受取れない場合の対策として有効です。

ポリシー違反後の消去： ポリシー違反によってロックされたコンピューターが、定められた一定時間内にロック解除されない場合、自動的に消去を実行します。

◆ BitLocker キー消去機能

管理サーバーからネットワーク経由で BitLocker キーの消去命令を送信することで、紛失したコンピューターの BitLocker キーを消去し、OS を起動不可能にする機能です。BitLocker キーを消去されたコンピューターは、回復キーを入力することで、再度利用可能となります。回復キーは管理サーバーからも確認することが可能です。

◆ リモートロック機能

管理サーバーからネットワーク経由でロック命令を送信することで、紛失したコンピューターを操作不能にする機能です。ロックされたコンピューターは管理サーバーからリモートでロック解除が可能です。

◆ 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コンピューターを操作不能にします。

◆ PC 情報の取得

コンピューターのハードウェア情報や OS 情報、アンチウイルスソフトの稼働状態やネットワーク情報を取得して表示することができます。

◆ 位置情報の取得

コンピューターの起動時、および、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。

◆ コンピューター一括管理

複数のコンピューターでご利用の場合、遠隔データ消去サービス管理サーバーから、すべてのコンピューター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 Home, Windows 11 Pro, Windows 11 Enterprise)
Microsoft Windows 10　(Windows 10 Home, Windows 10 Pro, Windows 10 Enterprise)

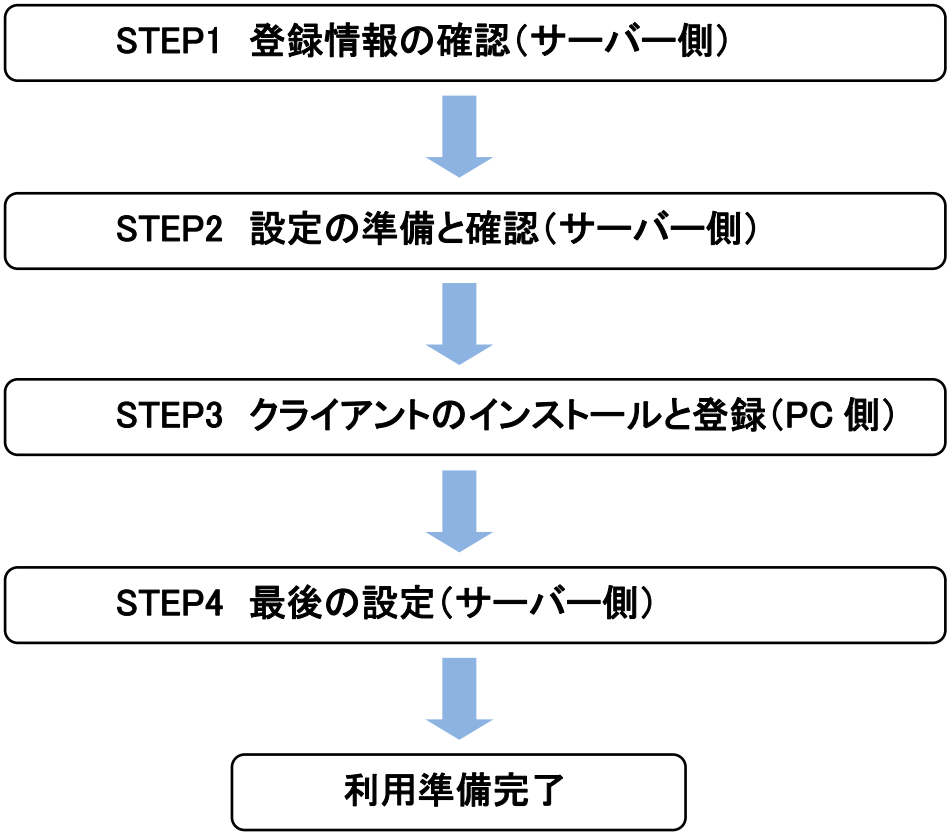
ハードウェア
CPU：1GHz 以上を推奨　(ARM アーキテクチャーには対応しておりません)
メモリ(RAM)：　2GB 以上を推奨
100MB 以上のハードディスク空き容量

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

※　本製品は、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。
※　本製品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。
※　製品の仕様は予告なく変更される場合があります。
※　本製品の利用登録、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コンピューター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://datawipeprm.nec-lavie.jp/admin/logindwp
   ※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。

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 二段階認証：該当IDの二段階認証を有効にする場合、スライドスイッチを ON にし**[保存]**ボタンをクリックします。二段階認証の詳細については「7.3 二段階認証」を参照してください。
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 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。

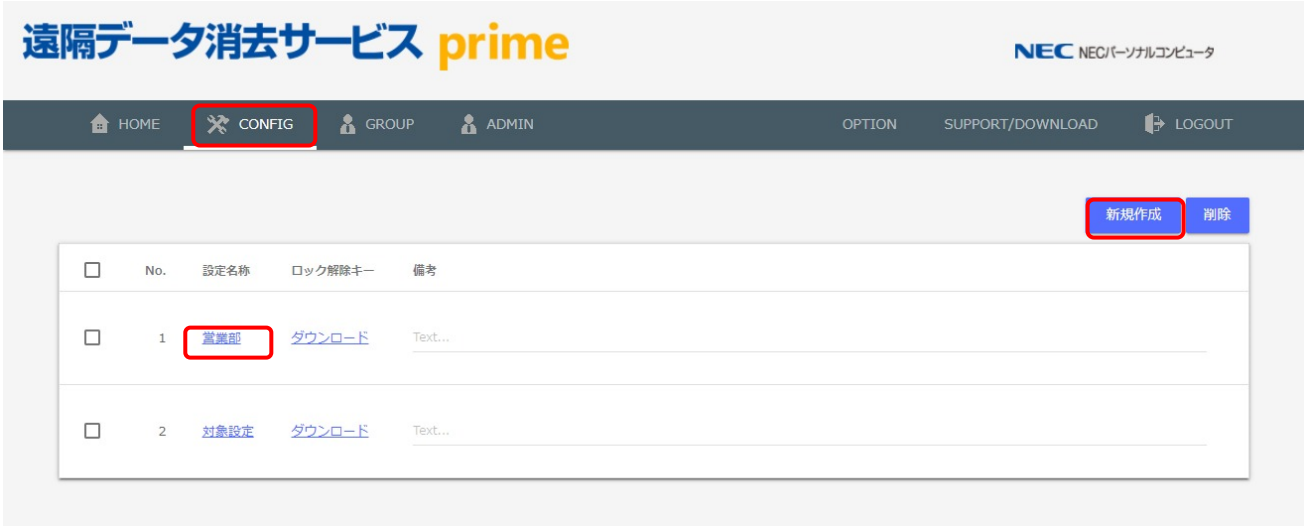
⑥ シリアル番号:クライアントプログラムの登録に必要な 8 桁のシリアル番号です。
⑦ 契約終了日:ご契約の終了日が表示されます。
⑧ 契約台数:お申込みいただいた台数が表示されます。
⑨ 登録台数:すでに登録済のコンピューターの台数が表示されます。
⑩ 管理者のメールアドレスを登録します。端末の登録完了時、消去実行時などにメール通知が行われます。
⑪ スマートフォンアプリの利用に必要な情報をダウンロードします。詳細については 7.2 項を参照してください。

※注意	・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。 ・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。 ・初期パスワードは速やかに変更することを推奨します。

STEP 2　設定メニューの準備

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。
監視対象となるコンピューター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・保存が可能です。



※ヒント	・コンピューター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。 ・どのコンピューター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。

基本設定

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コンピューター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 BitLocker 回復キー
BitLocker による暗号化を行っている場合、通常は PC 情報画面に回復キーが表示されます。(「7.2 PC 情報」を参照)BitLocker の回復キーを管理サーバーに送信したくない場合、「取得しない」を選択します。

※注意	・BitLocker 回復キーを「取得しない」設定にした場合でも、BitLocker キー消去命令を発行可能です。詳細は「4. BitLocker キー消去機能」を参照してください。 ・BitLocker キー消去を実行した場合、該当パソコンは BitLocker 回復キーを入力しない限り、起動できない状態となりますが、暗号化されたデータが HDD 内に残存する状態となります。BitLocker 回復キーを「取得しない」設定にした状態で BitLocker キー消去機能を使用する場合は、回復キーの管理状態に十分ご注意ください。 ・本機能を利用する場合、クライアントプログラムバージョン 3.0 以降をご使用ください。

⑤ 認証間隔
消去やロック命令の取得、新しいポリシーなど設定情報をサーバーから取得するためにコンピューターがサーバーにアクセスする通信間隔を選択します。5 分、15 分、30 分、60 分から選択できます。

⑥ 情報通知間隔
コンピューターの端末情報をサーバーに送信する通信間隔を選択します。6 時間、12 時間、24 時間から選択できます。

⑦ 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。

⑧　自動消去
コンピューターが一定時間サーバーと通信できない場合の制御を指定します。詳細は「2.2 自動消去」を参照してください。

ネットワーク関連ポリシー

⑨　オンライン／オフラインの監視
コンピューター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コンピューターに適しています。有線・無線接続に関わらずコンピューターがオンラインの時にロックは発動しません。

⑩　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コンピューターをロックします。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。コンピューター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。

⑪　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コンピューターをロックします。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。コンピューター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。

⑫　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：⑫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。

⑬　許可する無線 LAN の SSID
上記⑪または⑫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。

⑪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。
⑫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

⑭　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や許可されていない SIM カードに差し替えられた際にコンピューターをロックします。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。

■「SIM カードの有無を監視する」を選択した場合

SIM カードが認識できない場合にロックが発動します。

■「SIM カードの変更を監視する」を選択した場合

最初に認識した SIM カードとは異なる SIM カードを検知した場合にロックが発動します。

※重要	・クライアントプログラムバージョン 2.0.9 以前をご利用の場合、SIM カードの変更監視機能をご利用いただけません。 ・パソコンに内蔵された無線 WAN モジュールの SIM カードのみが監視対象となります。
※ヒント	・「SIM カードの変更を監視する」を指定する場合、管理者が許可する SIM を差した状態でポリシーを適用すれば、利用者が無断で SIM を交換した際にパソコンをロックすることが可能です。 ・「SIM カードの変更を監視する」を有効にしたパソコンの SIM を交換する必要がある場合、SIM カードの監視機能を無効にしたポリシーをパソコンに適用した状態で SIM の交換を実施してください。SIM 交換後に再度「SIM カードの変更を監視する」を有効にしたポリシーを適用すれば、交換後の SIM を許可対象と認識します。

コンピューターの利用エリア監視

⑮　コンピューターの位置情報の監視

コンピューターがあらかじめ指定した利用エリアから外に出た時にコンピューターをロックします。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コンピューターに適しています。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

⑯　操作ロック実行中の画面表示
ロックの実行時にコンピューター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	・ご利用のコンピューター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。表示がこの状態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ます。 ・操作ロック中に表示されるメッセージを指定してあっても、ロック命令（3.1 項参照）によるロック発動時には、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。

⑰　ロック時のアラーム
[ロック実行時にアラームを起動する]を ON にするとロック発動時にアラーム音を鳴らすことができます。ロックが解除されるとアラームも停止します。

※注意	・アラーム音は内蔵スピーカの最大出力と同等の音量です。機種によって最大音量は異なります。また、アラームが実行された後のコンピューターは、音量設定が最大音量になっている場合がありますのでご注意ください。

⑱　ポリシー違反による操作ロック後の自動消去
本機能を ON にするとポリシー違反によるロックが発動後、指定した時間内にロックを解除しなければ自動でドライブの消去を実行します。詳細は「2.3 ポリシー違反後の消去」を参照してください。

Windows ログオンパスワードの監視

⑲　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コンピューター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。

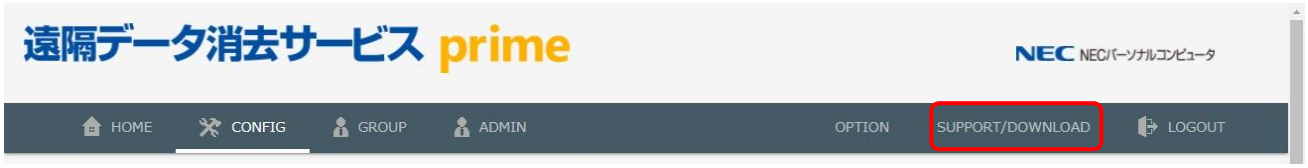
※注意　本ポリシーに違反した時のアクションは強制シャットダウンのみです。他のポリシーのようにロックアクションを選択・実行はできません。

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	・本製品では最大 10 個の監視ポリシーを作成できます。複数のコンピューター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利用登録

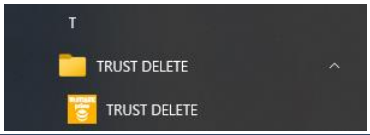
1. 管理サイトにログインして左メニューの SUPPORT/DOWNLOAD 画面を開きます。



2. 別ウインドウでサポートページが開いたら、最新版クライアントプログラムの[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コンピューターに保存します。

3. 管理対象のコンピューター上で、取得したインストールプログラム（TDPrimeInst.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。

4. クライアントプログラムのインストール作業が完了したら、プログラムメニューから**[TRUST DELETE]**を実行してください



5. TRUST DELETE 登録ツールが起動したら、シリアル番号欄に 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を変更してから、**[登録]**ボタンをクリックして利用登録を行ってください。「登録が完了しました」と表示されたらクライアントの利用準備は完了です。

   ※シリアル番号は STEP1の⑥をご参照ください。ライセンス証書に記載のライセンス番号とは異なりますのでご注意ください。

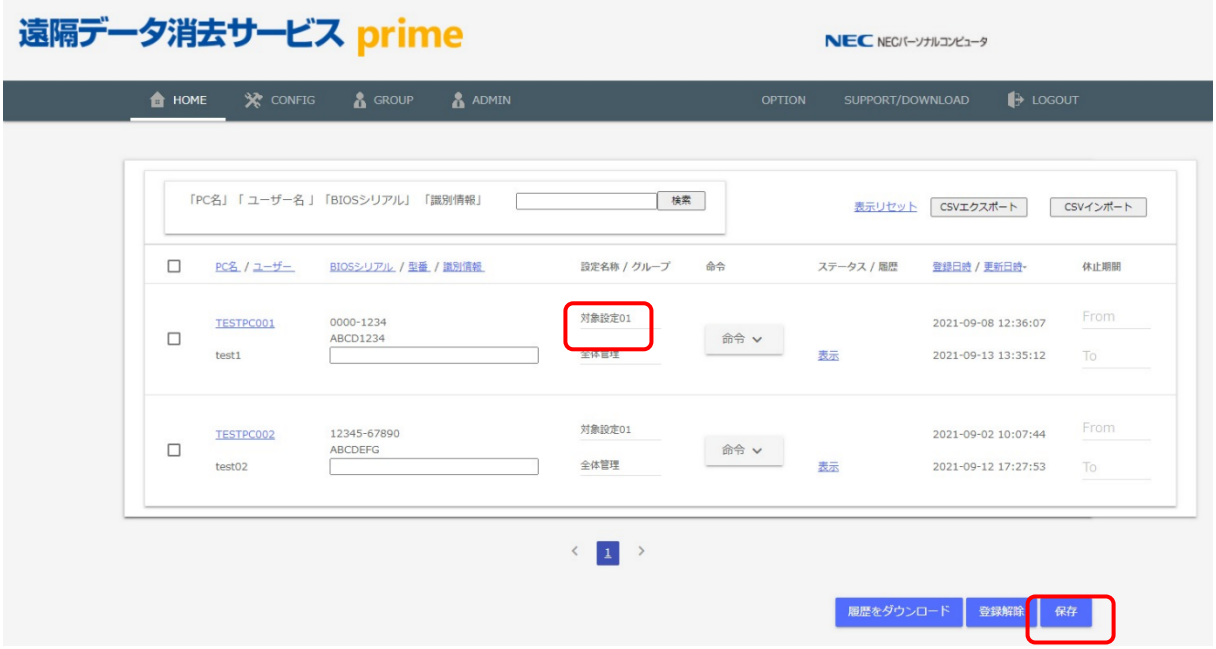
※重要	・インストール完了後は必ずコンピューターを再起動してください。 ・利用登録を完了しなければ本プログラムは正しく動作しません。必ず利用登録を行ってください。

STEP 4　クライアントプログラムの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. 登録したコンピューターがリストに表示されていることを確認してください。
各コンピューターの**[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コンピューターに同じ設定（設定番号1）が適用されています。コンピューター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。



※重要	・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認証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、TRUST DELETE 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、対象のコンピューターを特定しやすくできるように、コンピューターの管理番号や、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 PC に異なるポリシーを一括して適用することも可能です。詳細は「6.1 CSV インポート」を参照してください。

STEP 5　利用者への告知

以上で遠隔データ消去サービス prime 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、貴社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て以下の 2 点が重要となります。

- 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
- 事故端末がオフライン状態であることによって命令を実行できない場合に備え、自動消去機能（2.2 項）やポリシー監視機能（2.3 項）を活用する

2．コンピューター紛失時のデータ消去

2.1　消去命令

万一コンピューターを紛失した際は、以下の手順に沿ってコンピューター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、対象となるコンピューターがネットワークに接続できることが条件となります。

※重要	・クライアントプログラムバージョン 1.0.47 以前をご利用の場合、本機能は UEFI 起動のコンピューターでのみご利用可能です。レガシーBIOS 環境では消去命令がグレーアウトして消去を実行することができません ・Microsoft Surface シリーズなどの一部機種では、UEFI セットアップ画面のセキュアブートの設定において[Microsoft Only] [Microsoft & 3rd party CA] [None]の選択が可能な場合があります。 [Microsoft Only]が選択されている場合には消去が実行できませんので、セキュアブートの設定は[Microsoft & 3rd party CA]または[None]を指定してください。

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 画面で紛失したコンピューターをコンピューター名や BIOS シリアル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

対象となるコンピューター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。

消去命令が発行されると、命令ボタンが**[キャンセル]**に変わります。
※この段階では消去を取り消すことができます。

該当コンピューターが管理サーバーと認証通信を行うと、消去命令を取得しドライブ消去が発動します。ステータスが消去完了に変わります。
※ステータスが消去完了と表示されると命令の取り消しはできません。

※注意	・消去命令を発行してもコンピューターが管理サーバーと認証通信するまでは消去は開始されません。 ・消去命令がコンピューターに送信されるタイミングでステータスは[消去完了]になります。この時点ではコンピューター側の消去が開始されたばかりで実際に消去が完了するまでには時間を要します。
※ヒント	・クライアントプログラムバージョン 2.0.6 以降を使用する場合、Phoenix Secure Wipe™に対応する VAIO 社製 PC では、ハードウェアと連携した消去を実行することで、ドライブ内の全てのデータをより確実に消去します。 対象となる PC は、HOME 画面上に Phoenix Secure Wipe™対応を示すアイコンが表示されます。 Phoenix SecureWipe™ 対応

消去命令をキャンセルする

HOME 画面で該当コンピューターのステータスが消去発行中であることを確認してください。命令ボタンをクリックして**[キャンセル]**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。

命令がキャンセルされ、ステータスがキャンセルに変わります。
しばらくするとステータスは空白に戻ります。

※重要	ステータスが消去発行中の間は命令をキャンセルできます。ステータスが消去完了になるとキャンセルできません。

2.2　自動消去

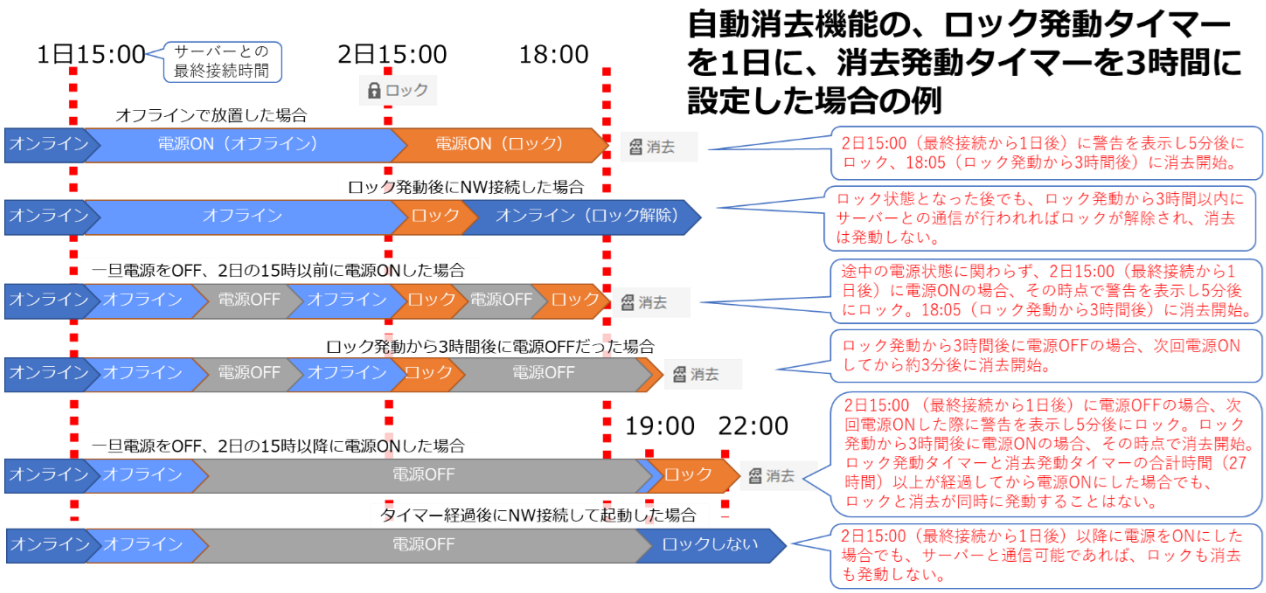
管理サーバーと通信ができない状態で一定時間が経過すると、時限爆弾のようにクライアントプログラムが能動的に消去を実行する機能です。通常、無線 WAN に対応した機種で、SIM カードを使用したインターネット接続が可能な場合を除き、盗難や紛失にあったパソコンが管理サーバーと通信可能な状態になる可能性は低いため、遠隔命令が受信・実行される可能性は極めて低いと言えます。
本機能を有効にすることで、紛失したコンピューターが管理サーバーからの消去命令を受取れない状況でも、クライアントプログラム側の判断でドライブ全体の消去を実行可能です。

※重要	・クライアントプログラムバージョン 1.0.47 以前をご利用の場合、本機能は UEFI 起動のコンピューターでのみご利用可能です。レガシーBIOS 環境では、消去は実行されず、ロックの解除が不可能な状態となります。 ・Microsoft Surface シリーズなどの一部機種では、UEFI セットアップ画面のセキュアブートの設定において[Microsoft Only] [Microsoft & 3rd party CA] [None]の選択が可能な場合があります。 [Microsoft Only]が選択されている場合には消去が実行できませんので、セキュアブートの設定は[Microsoft & 3rd party CA]または[None]を指定してください。

自動消去の実行条件

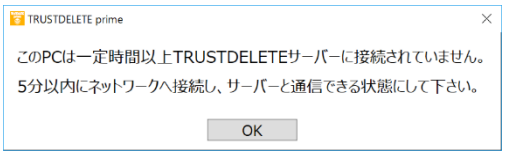
あらかじめ管理サーバーでロックが発動するまでの時間と消去が発動するまでの時間を指定します。指定した時間より長い間、コンピューターがインターネットに接続しない状態が続くと、まずロックが発動します。ロックが発動してから、さらに指定した時間インターネットに接続しない状態が続くと消去が開始されます。電源 OFF の間やスリープ中もタイマーはカウントを続けています。タイマー設定時間に達する前に、インターネットに接続し、管理サーバーとの認証通信が行われると、その時点でタイマーがリセットされ、タイマーはゼロから再開されます。また、USB 解除キーを使用して、一時的にロックを解除することも可能です。USB 解除キーを使用するには、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てください。ロック実行後に USB キーをパソコンに挿すことで、一時的にロックが解除されます。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。保護対象の機器の 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。



設定方法

CONFIG 画面で任意の設定名称をクリックし、設定の編集画面を開きます。「自動消去」の項目で**[自動消去を有効にする]**を ON にすると自動消去機能が有効になります。



[ロック発動までの時間]を 1 日、2 日、3 日、1 週間、2 週間から選択します。選択した時間以上、インターネットにつながらない状況が続くと警告を表示し、5 分以内にサーバーと通信できない場合はコンピューターをロックします。

[ロック発動後に消去を開始するまでの時間]を 1 時間、2 時間、3 時間、1 日、2 日、3 日、1 週間から選択します。コンピューターがロックされてから、選択した時間以上インターネットにつながらない状況が続くと消去を開始します。

コンピューターの利用頻度に応じて適切な設定時間を選択してください。

※以上の設定を行った後、必ず画面右下の**[保存]**ボタンをクリックしてください。

重要事項 （必ずお読みください）

- ◆ 不測の事態により、誤ってロックや消去が発動することを防ぐために、コンピューターの起動時には猶予期間を設けています。ロックや消去の発動タイマー時間を経過しても、コンピューターの起動から猶予期間内（ロックの猶予は 5 分、消去の猶予は 3 分）にネットワークに接続し、サーバーと認証通信が行われると、ロックや消去は発動しません。
- ◆ タイマー時間を過ぎると、コンピューターが起動、またはスリープや休止から復帰したタイミングで（猶予期間内に認証しなければ）ロックまたは消去が実行されます。本機能を解除するにはロック・消去の発動タイマーが指定時間に達する前にコンピューターをインターネットに接続し、サーバーと通信可能な状態にしてください。不測の事態により、指定時間より長い期間コンピューターを放置していた場合、あらかじめコンピューターをネットワークケーブルに接続するなど、速やかにサーバーと通信可能な状態で起動してください。
- ◆ コンピューターをオフラインで起動したまま長時間放置していた場合、指定した時間が経過した時点でロックや消去が実行されますのでご注意ください。

◆ コンピューターの時刻が正しくないと自動消去が発生する場合があります。自動消去をご利用になる前に必ずコンピューターの日付と時刻が正確か確認してください。コンピューターの時刻をインターネット時刻と同期しておくことをおすすめします。
◆ 本機能をご利用になる場合は、時間設定およびコンピューターの使用方法についてくれぐれもご注意ください。紛失が発生しなくても予期せぬ事態によりコンピューターを使用できないケースが起こりえます。タイマー時間は余裕をもって設定してください。
◆ コンピューターの修理や復元、長期保管を行う際は、該当コンピューターに対して自動消去を無効にした設定を事前に適用してください。
◆ ロック発動前の警告はログオン後に表示されます。ログオンまでに時間がかかった場合などには、警告の表示前や表示直後にロックが発動する場合があります。
◆ 本機能を有効にする場合、コンピューターの利用者に対して、自動消去の機能と実行条件について十分な説明を行ってください。

※自動消去の機能と実行条件について十分ご理解の上でご利用ください。

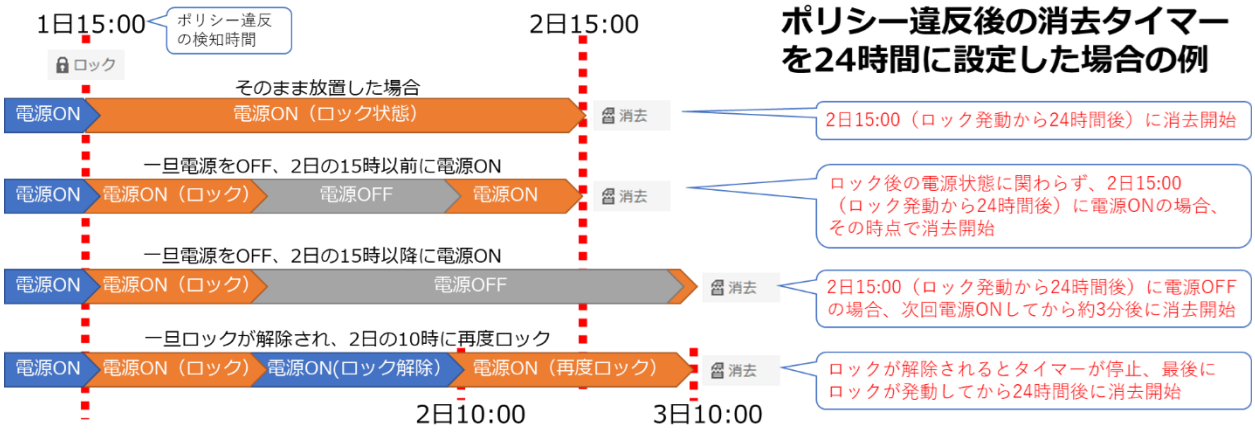
2.3　ポリシー違反後の消去

ポリシー違反でコンピューターがロックされたのち、違反状態が一定時間継続するとドライブ消去を実行する機能です。
紛失したコンピューターが管理サーバーからの消去命令を受取れない状況で、消去を実行するための条件をより柔軟に指定できるため、データを悪用されるリスクをさらに軽減します。

※重要	・クライアントプログラムバージョン 1.0.47 以前をご利用の場合、本機能は UEFI 起動のコンピューターでのみご利用可能です。レガシーBIOS 環境では、消去は実行されず、ロックの解除が不可能な状態となります。

ポリシー違反後の消去実行条件

管理サーバーでポリシー違反後の消去タイマー時間を設定します。コンピューターがロックされるとタイマーが作動します。タイマーの時間内にロックを解除できなければ消去を実行します。電源 OFF の間やスリープ中もタイマーはカウントを続けています。ロックを解除するとタイマーが停止します。



設定方法

CONFIG 画面で任意の設定名称をクリックし、設定の編集画面を開きます。
[ロックのポリシー]の項目で**[ポリシー違反による操作ロック後の消去]**を ON にし、消去が発動するまでの時間を、スライダーを操作し 1 時間から 168 時間までの間で指定します。ポリシー違反によるロックが発動した後、指定した時間内にロックを解除しなければドライブの消去を開始します。

※以上の設定を行った後、必ず**[保存]**ボタンをクリックしてください。

※重要	ポリシー違反によるロックと自動消去機能によるロックでは、それぞれ解除方法が異なります。正しい方法でロックを解除しなければ、指定時間の経過後に消去が開始されます。本機能を有効にする際は、ロックの解除方法を必ず事前に確認してください。 ポリシー違反によるロックを解除する方法は「3.2 ポリシー違反によるロック機能」を参照してください。

重要事項 （必ずお読みください）

◆ 不測の事態により、誤ってロックや消去が発動することを防ぐために、コンピューターの起動時には猶予期間を設けています。消去の発動タイマー時間を経過しても、コンピューターの起動から 3 分以内に、ポリシー違反状態を解消する、ロック解除キーを使用するなどして、ロックが解除されると、消去は発動しません。

◆ タイマー時間を過ぎると、コンピューターが起動、またはスリープや休止から復帰したタイミングで（3分以内にロックを解除しなければ）消去が実行されます。本機能を解除するには消去の発動タイマーが指定時間に達する前にロックを解除してください。不測の事態により、指定時間より長い期間コンピューターを放置していた場合、あらかじめ、サーバー側で該当コンピューターに対してポリシー監視を無効にした設定を適用するなどした上で、該当コンピューターをネットワークケーブルに接続するなど、速やかにサーバーと通信可能な状態で起動してください。

◆ コンピューターをポリシー違反状態で起動したまま長時間放置していた場合、指定した時間が経過した時点で消去が実行されますのでご注意ください。

◆ コンピューターの時刻が正しくないと自動消去が発生する場合があります。自動消去をご利用になる前に必ずコンピューターの日付と時刻が正確か確認してください。コンピューターの時刻をインターネット時刻と同期しておくことをおすすめします。

◆ コンピューターをロック状態で長時間放置しておくと、次回起動時に自動消去が実行される可能性がありますのでご注意ください。

◆ 本機能のご利用にあたってはタイマー時間の設定についてくれぐれもご注意ください。紛失が発生しなくても予期せぬ事態によりコンピューターを使用できないケースが起こりえます。タイマー時間は余裕をもって設定してください。

◆ コンピューターの修理や復元、長期保管を行う際は事前に本機能を無効にしてください。

◆ 本機能を有効にする場合、コンピューターの利用者に対して、ロックの解除方法、ならびにポリシー違反後の消去実行条件について十分な説明を行ってください。

※本機能と実行条件について十分ご理解の上、ご利用になるようご注意ください。

3． ロック機能

ロック機能はマウス、キーボード、タッチパネル等の入力デバイスを無効化してコンピューターを操作不能にします。いったんロックを実行すると再起動後も操作不能です。
コンピューターをロックするにはロック命令とポリシー違反によるロックの 2 通りがあります。

3.1　ロック命令

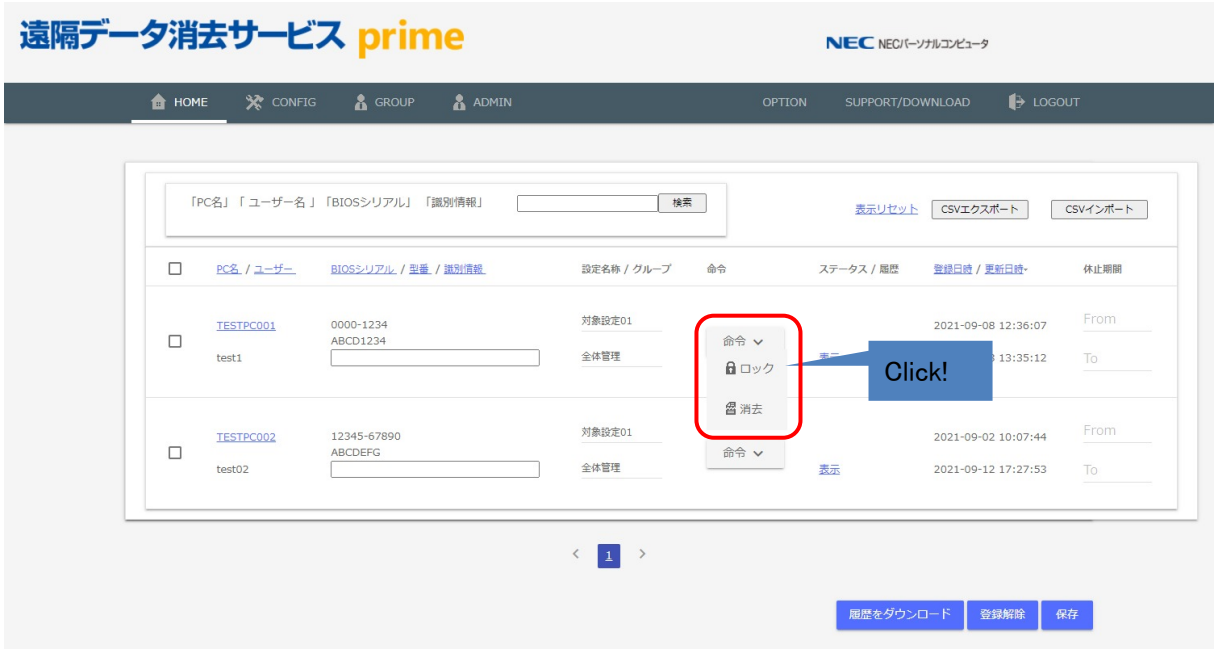
管理サーバーからの命令でロックやロック解除を実行します。対象となるコンピューターがネットワークに接続できることが条件となります。

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コンピューターをコンピューター名や BIOS シリアル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

対象となるコンピューターの命令ボタンをクリックして[**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。



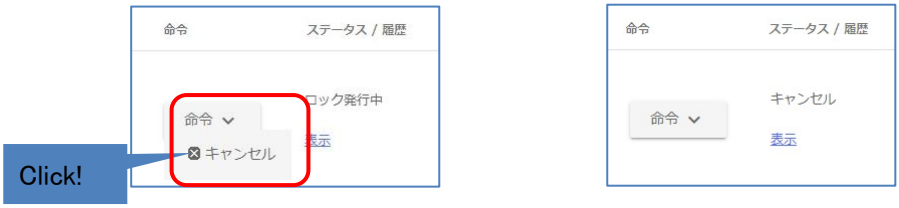
ロック命令が発行されると、命令ボタンがキャンセルに変わります。
該当コンピューターが管理サーバーと認証通信を行うと、ロック命令を取得しロックが発動します。ステータスがロック完了に変わります。

※注意	・ロック命令やキャンセル命令を発行してもコンピューターが管理サーバーと認証通信するまでは実際にはロックまたはロック解除されません。 ・消去命令を発行するとロック命令は発行できなくなります。消去命令をキャンセルするとロック命令が発行可能になります。ロックが発動していても消去命令を発行すればドライブ消去が発動します。

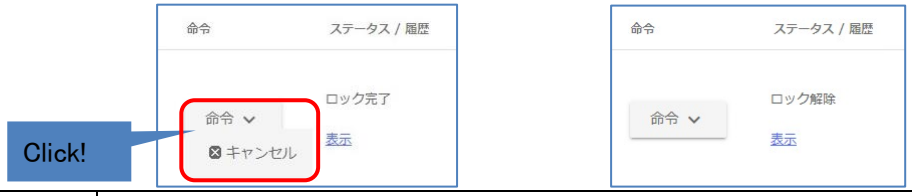
STEP3 ロック命令の解除

ロック命令を解除するには、ロック命令をキャンセルします。
HOME 画面で該当コンピューターのステータスがロック発行中である場合、該当コンピューターはロック命令を受信していません。

命令ボタンをクリックして[**キャンセル**]をクリックし、確認画面が表示されたら[OK]をクリックします。
ロック命令が取り消され、ステータスがキャンセルに変わります。しばらくするとステータスは空白に戻ります。



HOME 画面で該当コンピューターのステータスが[ロック完了]である場合、該当コンピューターはすでにロック命令を受信し、ロックされています。
命令ボタンをクリックして[**キャンセル**]をクリックし、確認画面が表示されたら[OK]をクリックします。
ロック命令が取り消され、ステータスがロック解除に変わります。該当コンピューターが管理サーバーと認証通信を行うとロックが解除され、ステータスは空白に戻ります。



※注意	ロック命令でロックされた端末は、後述の USB 解除キーでは解除できません。

3.2 ポリシー違反によるロック

コンピューター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自動でロックを発動します。ポリシー違反による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、コンピューター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。ロック実行後に USB キーをコンピューター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. 遠隔データ消去サービス prime の基本セットアップ 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。保護対象の機器の 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コンピューター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コンピューターが管理サーバーにアクセスするまではコンピューター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ておいてください。 ・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。

4． BitLocker キー消去機能

一部の Microsoft Windows に搭載のハードディスク暗号化機能である BitLocker を使用している PC に対して、管理サーバーからの命令で BitLocker のキーを消去することで Windows が回復キーなしでは起動できない状態になります。対象となるコンピューターがネットワークに接続できることが条件となります。

4.1 動作条件

・システムドライブの BitLocker ドライブ暗号化が完了していること
・コンピューターに TPM が搭載され、TPM と回復キー（数字パスワード）のみを使用していること
・クライアントプログラムバージョン 1.1.16 以降を使用していること

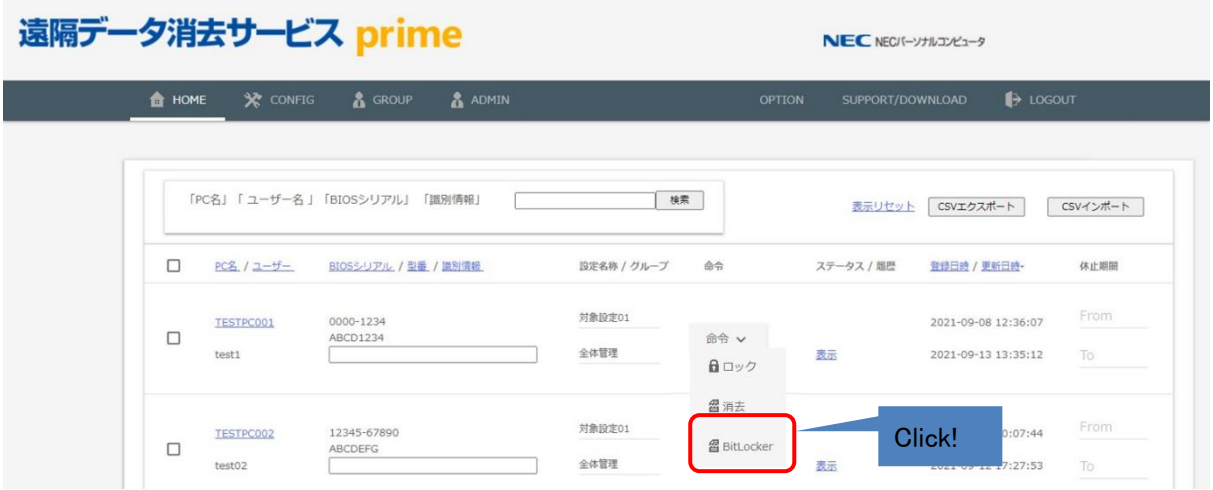
上記の条件を満たす PC は、「HOME」画面から対象となる PC の「PC 名」リンクを開いた際に表示される、「PC 情報ページ」にて、「BitLocker キー消去」項目が「有効」となり、ドライブごとの「BitLocker 暗号化」の状態、および「BitLocker 回復キー」が表示されます。

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コンピューターをコンピューター名や BIOS シリアル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 BitLocker キー消去命令を発行

対象となるコンピューターの命令ボタンをクリックして[BitLocker]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。



BitLocker キー消去命令が発行されると、命令ボタンが**[キャンセル]**に変わります。※この段階では消去を取り消すことができます。

該当コンピューターが管理サーバーと認証通信を行うと、命令を取得し BitLocker キー消去が発動します。ステータスが BL 消去完了に変わります。
※ステータスが BL 消去完了と表示されると命令の取り消しはできません。

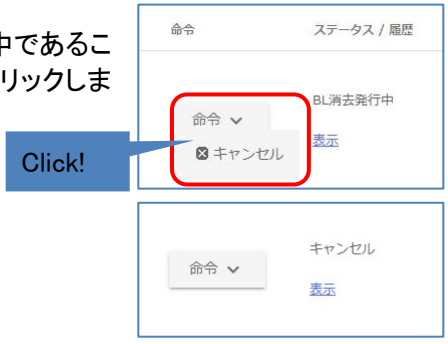
※重要	BitLocker キーの消去が完了すると（ステータスが「BL 消去完了」になると）、ロック命令や消去命令を発行することが可能となります。 しかし、該当コンピューターは回復キーを入力しない限り、起動できない状態となるため、通常は新たな命令を受け取ることができません。 つまり、紛失や盗難の際に BitLocker キーの消去を実行すると、ドライブの全消去を実行することが現実的に不可能となるため、データが HDD 内に残存し続けるリスクを伴います。 本機能をご使用する際は、消去命令を実行する必要がないか、慎重にご判断ください。

※注意	・BitLocker キー消去命令を発行してもコンピューターが管理サーバーと認証通信するまでは BitLocker キー消去は開始されません。 ・BitLocker キー消去命令がコンピューターに送信されるタイミングでステータスは[BL 消去完了]になります。 ・BitLocker キーの消去を実行した後で、パソコンを起動する際に必要となる回復キーは、「PC 情報ページ」で確認することができます。BitLocker 回復キーを取得しない設定にすることも可能（「1.STEP2 ④」参照）ですが、その状態で BitLocker キー消去命令を発行する場合には、回復キーが適切に管理されているか事前にご確認ください。

4.2 BitLocker キー消去命令をキャンセルする

HOME 画面で該当コンピューターのステータスが BL 消去発行中であることを確認してください。命令ボタンをクリックして**[キャンセル]**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。

命令がキャンセルされ、ステータスがキャンセルに変わります。
しばらくするとステータスは空白に戻ります。



※注意	・ステータスが BL 消去発行中の間は命令をキャンセルできます。ステータスが BL 消去完了になるとキャンセルできません。 ・BitLocker の回復キーを入力することでシステムを復号してコンピューターを起動できます。このあと BitLocker を解除するか再設定するまで、毎回起動時に回復キーの入力を求められます。 ・遠隔データ消去サービス prime は、「BitLocker ドライブ暗号化」に対応しています。「デバイスの暗号化」には対応していません。

５．消去やロック命令の進捗を確認するには

管理サーバーの HOME 画面で各コンピューターの状況を確認できます。

5.1 ステータス

コンピューターに対する命令の状態を表示します。

ステータス表示	命令の通達状況	クライアントの状態
空白	命令なし、またはロック解除状態	何も起きていません
消去発行中 (BL 消去発行中)	消去命令発行／命令は未達	何も起きていません
消去完了 (BL 消去完了)	消去命令発行／命令は到達	消去を実行中または消去完了
キャンセル	発行した命令のキャンセル (命令取り下げ)を発行中	何も起きていません
ロック発行中	ロック命令発行／命令は未達	何も起きていません
ロック完了	ロック命令発行／命令は到達	ロックを実行中
ロック解除	ロック解除命令発行／命令は未達	ロックを実行中

※注意	・ステータスは命令ボタンの操作の状態を表します。ポリシー違反によるコンピューターの(ロックや解除の)状態は履歴画面にのみ表示されます。 ・コンピューターが消去命令を受信するとステータスはすぐさま消去完了になります。しかし実際はコンピューター側で消去が実行開始された状態であり、消去が完了するまでには時間を要します。

5.2 履歴

[履歴]欄の**[表示]**リンクをクリックすると、該当端末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消去命令や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コンピューター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。

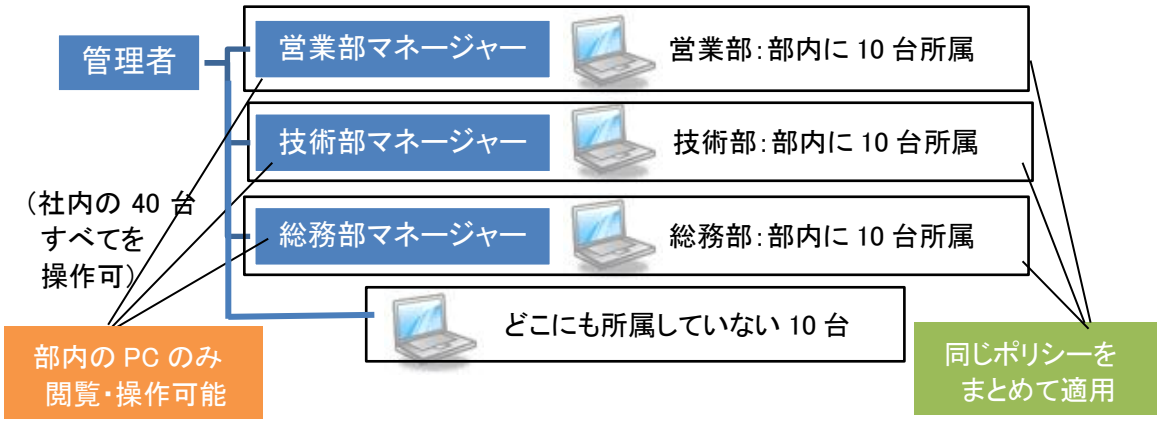
① 発動日時：ポリシー違反の発生日時、またはリモート命令の実行日時を表示します。
② アクション：ロック、ロック解除、消去など実行したアクションを表示します。
③ 発動理由：検出した違反の種類を表示します。
④ 端末情報：違反検出時のバッテリー残量や発動時にログオンしているユーザーの情報、コンピューターの位置情報を表示します。
⑤ ログイン ID：命令を発行した管理者の ID を表示します。

※ヒント	・パソコンの盗難や紛失が発生した際、アクション発動履歴またはリモート命令の実行完了履歴の「端末情報」に表示される「最終ログオン日時」が、事故発生の前か後か、「発動時のログオンユーザー」が事故発生時の状態から変わっていない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。 ・Windows の[アカウント] 設定の[サインインオプション]で、「更新または再起動の後にサインイン情報を使ってデバイスのセットアップを自動的に完了します。」や「更新後に自動的にセットアップを完了するには、サインイン情報を使用します」などの項目が「オン」になっている場合、サインインを行わなくとも「最終ログオン日時」や「発動時のログオンユーザー」が更新される場合があります。また、アクション発動時にログオフ状態だった場合、端末情報の「発動時のログオンユーザー」「最終ログオン日時」は表示されません。Windows の設定をご確認の上、事前に動作の確認を行うことを推奨いたします。
※注意	・無線 WAN に対応した機種で、SIM カードを使用したインターネット接続が可能な場合を除き、盗難や紛失にあったパソコンが管理サーバーと通信可能な状態となる可能性は低いため、一般的には事故後に発動したアクションの履歴情報は表示されません。

	・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コンピューターから受信した実行履歴の 2 つの履歴が表示されます。 ・位置情報は Windows の機能を利用して測定し記録します。 ・Windows が位置情報を取得できない場合、位置情報は表示されません。

6. グループ管理機能

企業（または組織）内で複数のコンピューター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コンピューター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、社内のコンピューター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	組織内のすべてのコンピューター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、消去命令の発行・キャンセル、消去履歴の閲覧等を実行することができます。
- ◆ グループを作成し、任意のコンピューター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コンピューターに対して、消去命令やロック命令の発行・キャンセル、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コンピューターの操作や閲覧はできません。
- ◆ 登録されているコンピューターの所属グループや設定の変更はできません。
- ◆ 登録されているコンピューターの登録解除、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、画面右下の**[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。

※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、組織内のすべての端末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。
※注意	・ログイン ID は 4～100 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。 ・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。

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コンピューター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。

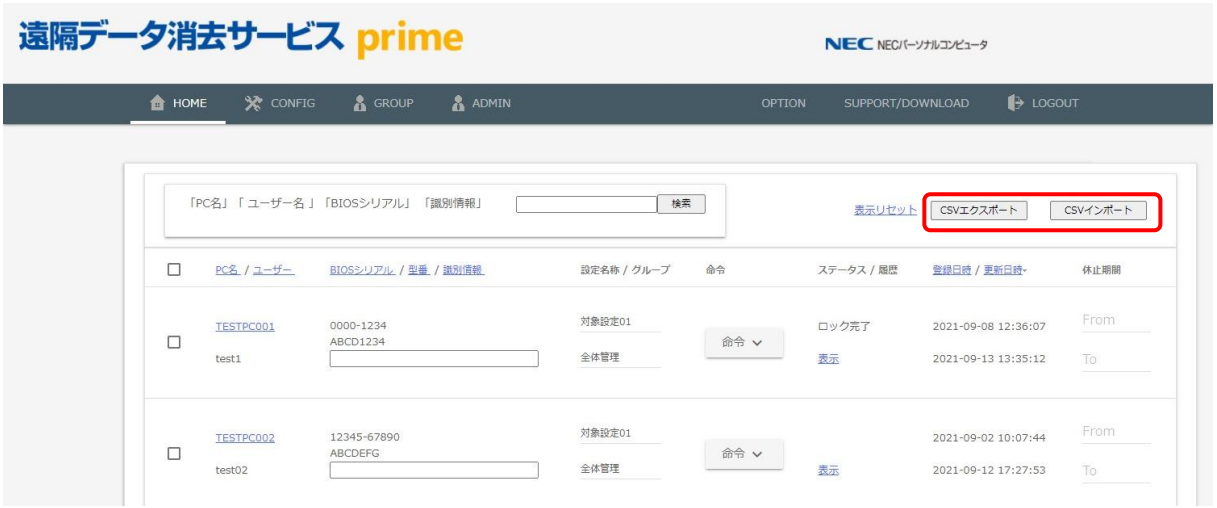
HOME 画面で対象コンピューターの**[グループ]**で、プルダウンから任意のグループ名を選択します。画面内で必要なコンピューターのグループ選択がすべて完了したら、画面右下の**[保存]**ボタンをクリックします。保存が完了すると、グループで指定された設定が反映さます。

※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。**多くのコンピューターを管理し、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コンピューターが管理サーバーと認証通信するまでは、以前の設定で監視を続けます。管理サーバーと認証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コンピューターに、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 PC 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「7.1 CSV インポート」を参照してください。

7．その他の機能

7.1 CSV インポート

「HOME」画面から CSV ファイルを使用してコンピューター一覧情報の取得、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、登録コンピューター情報の一覧を 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。コンピューター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、意図しない端末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	・一部のコンピューター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コンピューターの設定は変更されません。 ・CSV インポートを使用して、コンピューター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。 コンピューターごとに異なる設定を適用したい場合には、対象コンピューターの「グループ ID」に「１」を指定してください。

8.2 スマートフォンアプリ

企業や組織の管理者に代わり、管理対象パソコンを利用するユーザー自身（以降「利用者」と記載）が、利用中のパソコンに対して以下の操作を行うためのツールです。
① 「利用者が、自身で管理するパソコン」へ消去命令を発行
② 「利用者が、自身で管理するパソコン」へロック命令を発行
③ 「利用者が、自身で管理するパソコン」のステータスや位置情報の確認

利用者がスマートフォンアプリを使用する場合も、引き続き、管理コンソールから、該当パソコンの集中管理が可能です。つまり、スマートフォンアプリからの命令によってロックされたパソコンに対して、管理コンソールからロックを解除する、消去を実行するといったことも可能です。 なお、スマートフォンアプリから命令を発行した際の管理対象パソコンのふるまいや、管理コンソール上の画面遷移は、管理コンソールから命令を発行した際のふるまいと同様です。

8.2.1 利用開始手順

管理対象とするすべてのパソコンの登録が完了している状態で、ADMIN 画面の「スマホアプリ」項目内にある「ダウンロード」ボタンをクリックします。

登録用 csv（Users.csv）ファイルがダウンロードされたらファイルの内容を確認し、管理対象パソコンの「PC名」をもとに、対象のパソコンを管理する利用者に対して、「アカウント ID」と「端末識別子」をお伝えし、下記のサイトに従ってスマートフォンアプリの利用準備を行うよう、ご案内ください。
https://www.onebe.co.jp/support/primenpc/download/primenpc_mobile_app_manual.pdf

なお、利用者に対して誤った「端末識別子」を通知した場合、スマートフォンアプリで対象パソコンを登録できない場合や、他人が管理するパソコンが登録されてしまう場合がありますのでご注意ください。

8.2.2 登録用 csv ファイルの内容

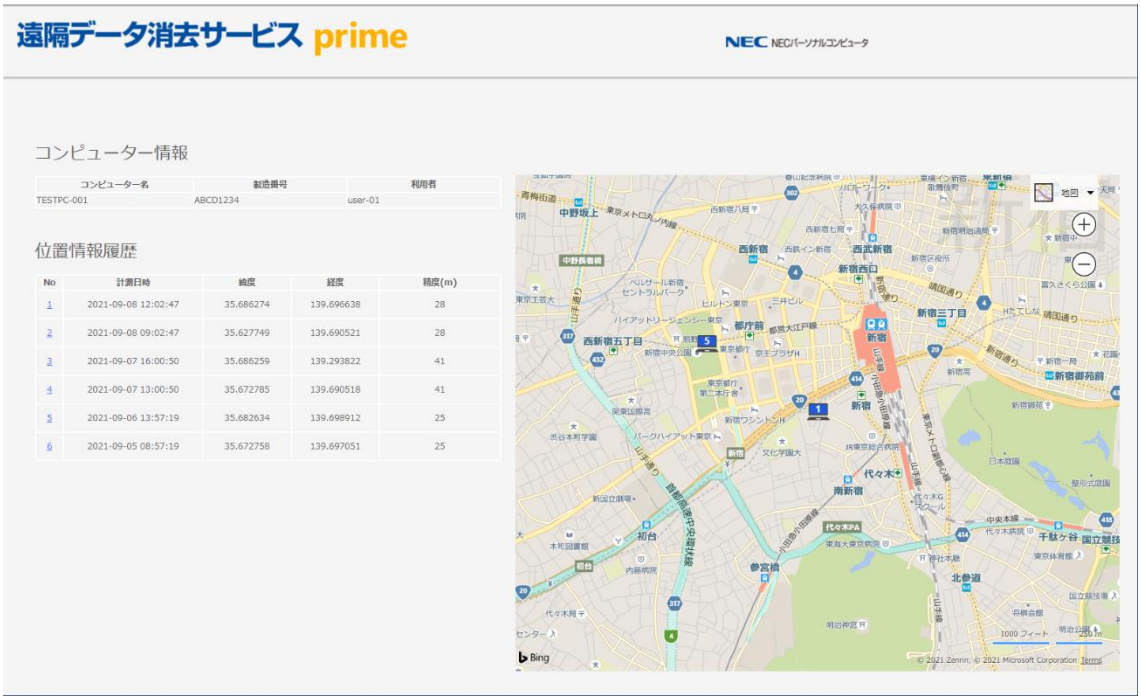
項目	記載例	内容
PC 名	TESTPC-001	管理サーバーに登録されたパソコンの PC 名です。この情報をもとに、該当パソコンを管理する利用者に端末識別子をお伝えください。
アカウント ID	ABCDEFG	契約組織を特定するための文字列。ライセンス契約ごとに一意な ID が付与されます。
端末識別子	123xyz	パソコンごとに一意となる識別用の ID です。スマートフォンアプリにこの情報を登録することで、利用者の管理対象パソコンを特定します。 スマートフォンアプリと端末識別子は 1 対 1 に紐づけられるため、1 つのパソコンを複数のスマートフォンで管理することも、1 台のスマートフォンで複数のパソコンを管理することもできません。
登録有無	登録済み	スマートフォンアプリの登録状況です。スマートフォンアプリの利用準備が既に完了しているパソコンの場合、「登録済み」と表示されます。

8.3 PC 情報と位置情報

パソコンのハードウェア情報や OS 情報、アンチウイルスソフトの稼働状態やネットワーク情報などを表示します。表示内容は CONFIG 画面で設定された情報通知間隔（6～24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。

② 位置情報
コンピューターを使用した位置情報の履歴を地図上で確認する機能です。コンピューターが稼働し、インターネットに接続された際に位置情報を取得します。管理サーバーとの通信が行われるまでは、サーバー上では表示されません。
「位置情報」ボタンをクリックすると別ウィンドウで地図が表示され、管理サーバーが受信した直近の 20 件の位置情報履歴が表示されます。



※注意	・位置情報は GPS 機能を搭載するコンピューター、または Windows8 以降の無線 LAN 機能を搭載するコンピューターで取得可能です。この画面には、違反を検出したタイミングで測定された位置情報は表示されません。 ・Windows が位置情報を取得できない場合、位置情報は表示されません。

8.4 二段階認証

管理コンソールをより安全に利用するため、ログイン時にメールによるワンタイムパスワード（認証コード）を併用した二段階認証を行います。本機能を有効にする場合、ADMIN 画面で該当IDの**[二段階認証を有効にする]**のスライドスイッチを ON にし**[保存]**ボタンをクリックします。

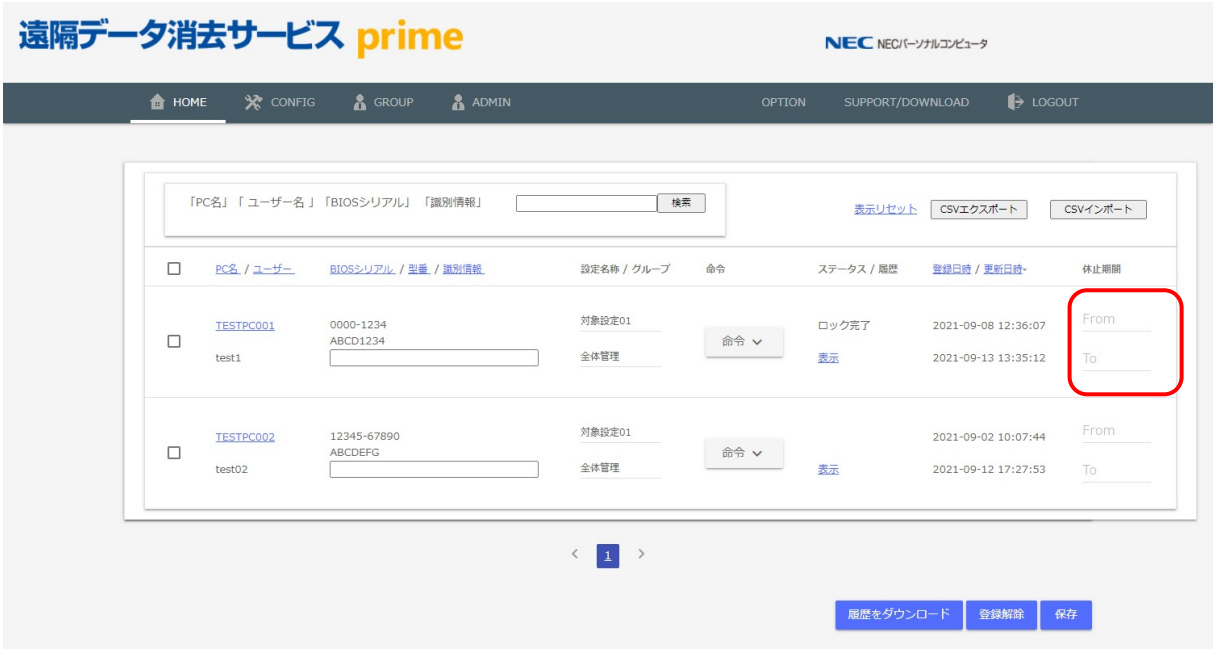
該当メールアドレス（ログイン ID）に送信される確認メールに記載された URL をクリックすると、該当するログイン ID で二段階認証が有効となり、次回以降のログインの際には、メールに記載されたワンタイムパスワード（認証コード）の入力が必要となります。

※注意	・確認メールに記載された URL の有効時間は 6 時間です。6 時間以内にクリックされない場合、該当 ID の二段階認証は無効となります。 ・ワンタイムパスワード（認証コード）の有効期限は 10 分間です。10 分以内にワンタイムパスワードが入力されない場合、ログイン画面に戻ります。 ・二段階認証が有効な状態のログイン ID（メールアドレス）は変更できません。ログイン ID（メールアドレス）を変更する場合は、二段階認証を一旦無効にしてください。

8.5 休止期間

HOME 画面の**[休止期間]**に開始日と終了日を入力すると、その期間はコンピューターがポリシーに違反してもアクションを実行しません。休暇や出張等の理由で、一定期間ポリシー監視を行いたくない場合にご利用ください。開始日と終了日を入力したら、必ず**[保存]**ボタンをクリックしてください。

◆ 休止の開始時刻：入力した日付の 0:00
◆ 休止の終了時刻：入力した日付の 23:59



※注意	・ポリシー違反によるロック実行中に休止期間が始まると、期間中は一時的にロックが解除されます。休止期間終了時にポリシー違反の状態であれば再びロックが発動します。 ・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。

8.6 コンピューターの登録解除

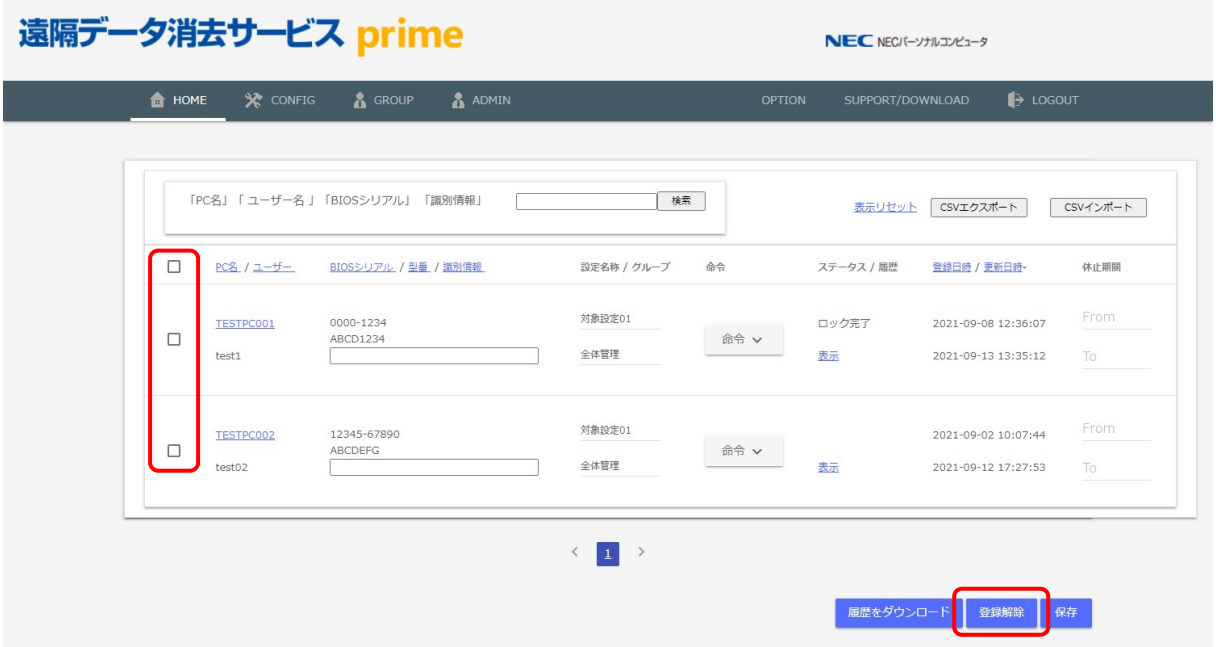
次のような場合は登録済みのコンピューターを登録から外す（登録解除といいます）必要があります。

- ◆ 新しい PC に買い換えた場合
- ◆ 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
- ◆ 契約台数が不足して登録台数に空きが必要な場合

登録解除の手順

HOME 画面で対象コンピューター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。以上でこのコンピューターの登録が抹消され 1 台分の空きができます。

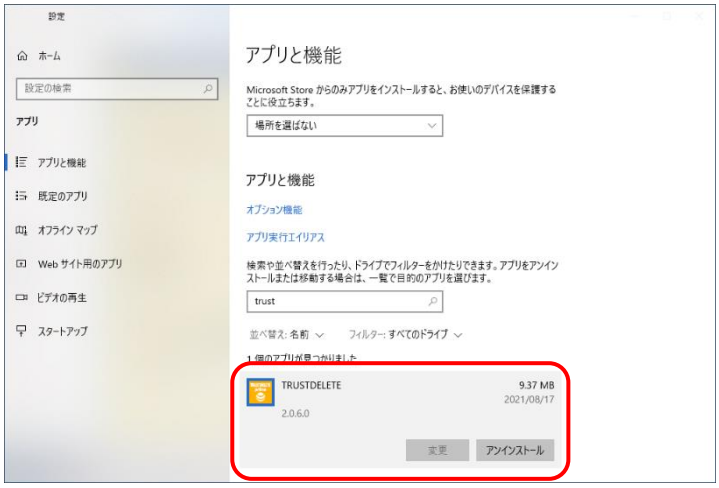
※注意	・管理サーバー側で登録解除を完了した後で、管理サーバーとの通信を行ったコンピューターでは、遠隔データ消去サービス prime の全機能が停止します。 コンピューターを紛失した際、「ポリシー違反後の消去」機能や「自動消去」機能を設定されていても、登録解除を行うと、消去が発動しない場合があります。 コンピューターを紛失した際には、「消去命令」または「ロック命令」を発行し、命令の実行が確認できるまで、対象コンピューターの登録解除は実施しない事を推奨いたします。 ・登録解除を行ったコンピューターの履歴情報およびデータ適正消去実行証明書は管理サーバーから削除されます。登録解除後も履歴情報やデータ適正消去実行証明書を保管しておく必要がある場合には、登録解除を実施する前に「8.1 CSV エクスポート」、または「7.2 証明書の発行」により、必要な情報を保存してください。



※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。

8.7 クライアントプログラムのアンインストール

監視対象コンピューター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、対象コンピューターで[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。



アンインストールパスワードをたずねられたら管理コンソールで指定されたアンインストールパスワード（P9 の②参照）を入力してください。

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コンピューターでは、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。