



TRUST DELETE Biz 管理サーバーマニュアル

- Ver.8.3.5-

ワンビ株式会社

はじめに

このたびは、TRUST DELETE Biz 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遠隔操作で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。

このマニュアルは、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
スタンダード版(for VAIO PC を含む)をご利用の方 <https://onebe.trustdelete.biz/>
for FUJITSU をご利用の方 <https://onebe.trustdelete.biz/loginfj>
- ✓ 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。

Microsoft Windows, Microsoft Windows 8.1, Windows 10, Windows 11, Microsoft Internet Explorer, Microsoft Edge は、米国 Microsoft 社の米国およびその他の国における登録商標です。本文中のその他の会社名および商品名は、各社の商標または登録商標です。

TDB202201215

目次

はじめに	2
トラストデリートとは.....	5
■サービス概要	5
■主な機能.....	5
■システム動作環境	6
1. トラストデリートサービスの基本セットアップ	7
STEP1 登録情報の確認	8
STEP2 設定メニューの準備	9
STEP3 クライアントプログラムのインストールと利用登録	12
STEP4 クライアントプログラムの登録確認と最後の設定	13
STEP 5 利用者への告知	15
2. コンピューター紛失時の消去命令の発行	16
STEP1 管理サーバーにログイン	16
STEP2 対象設定の確認	16
STEP3 消去命令を発行	16
消去命令をキャンセルする	17
3. 自動消去機能	18
自動消去の実行条件	18
設定方法	18
どのフォルダーを消去するか	18
重要事項（必ずお読みください）	19
4. BitLocker キーの消去	20
動作条件	20
設定方法	20
5. 不可視機能	21
不可視機能とは	21
どのフォルダーが不可視になるのか	21
不可視機能の実行タイミング	21
不可視機能を有効にするには	21
不可視の解除その1: ネットワーク認証	21
不可視の解除その2: 手動解除	21
6. リモートロック機能	22
STEP1 管理サーバーにログイン	22
STEP2 対象設定の確認	22
STEP3 リモートロック命令を発行	22
STEP4 リモートロックの解除方法	23
オフライン状態でリモートロックを一時的に解除する方法	23

7. タイマーロック機能	25
ロックの実行条件	25
設定方法	25
解除方法	25
8. 消去やロック命令の進捗を確認するには	28
発動条件とステータス	28
ステータスの解説	28
消去命令またはリモートロック/リモートアンロックの完了時	29
9. 位置情報取得機能	30
動作条件	30
設定方法	30
位置情報の確認方法	30
10. グループ管理機能	32
グループ管理機能とは	32
グループ管理機能でできること	32
管理者とグループ責任者の権限の違い	32
グループ管理機能を使う前の準備	33
所属グループの指定方法	34
所属部署を決定または変更するときの注意事項	34
11. その他の機能	35
ログイン時間制限	35
コンピューター検索機能	35
ソート機能	35
コンピューターの登録解除	35

トラストデリートとは

■ サービス概要

本サービスはコンピューター内のデータを遠隔操作で消去できるサービスです。コンピューターに専用プログラムをインストールすることによって、万一の盗難・紛失時に、ネットワーク経由で命令を発行して、失くしたコンピューターのデータを消去することができます。また、コンピューターがネットワークに接続できない状況では、不可視機能やロック機能、自動データ消去機能をご利用になることでコンピューター内のデータを保護することができるので安心してお使い頂けます。

■ 主な機能

◆ データ消去

コンピューターの盗難・紛失時に、管理サーバーからネットワーク経由で消去命令を送信することで、紛失したコンピューター内のデータを消去する機能です。命令を受信するためには紛失したコンピューターがインターネットに接続される必要があります。インテル®スマートコネクテクノロジー対応のコンピューターでは、スリープ中にインターネット接続を検出して、消去命令の受信および消去の実行が可能です。

◆ データ不可視

コンピューターがオフラインで管理サーバーからの命令を受信できない状況下で、一時的にデータを隠匿してデータを保護する機能です。不可視になったデータは元に戻すことが可能です。

◆ 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。

◆ タイマーロック機能

コンピューターが一定時間インターネットに接続できない状況が続くと、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する機能です。

◆ 自動データ消去

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する機能です。本機能は消去命令を管理サーバーから取得する必要がないため、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の消去に有効です。

◆ 位置情報取得

コンピューターの位置情報を 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、トラストデリート管理サーバーから、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)

Microsoft Windows 8.1 (Windows 8.1, Windows 8.1 Pro, Windows 8.1 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いません)

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 Internet Explorer 11 を推奨

Microsoft Edge

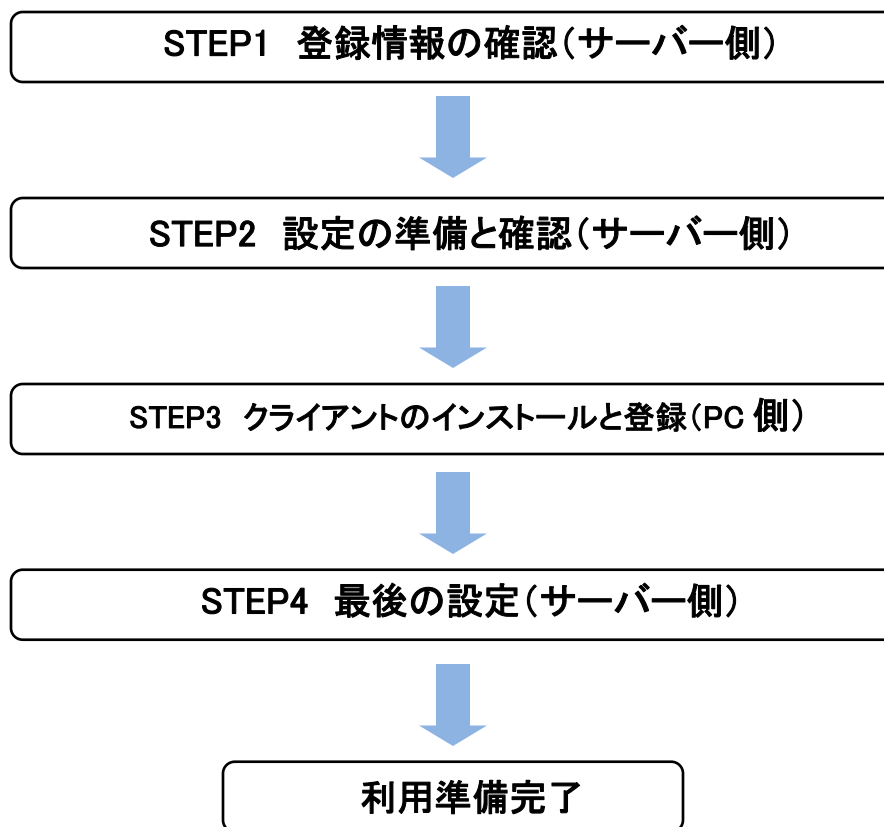
Google Chrome

- ※ 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、メールの送受信などのご利用には、インターネット接続環境が必要です。

1. トラストデリートサービスの基本セットアップ

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。

クライアントプログラムのセットアップはクライアントマニュアルを参照してください。



STEP1 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 Internet Explorer)から次の URL にアクセスし、管理サーバーにログインします。
 スタンダード版 (for VAIO PC を含む) をご利用の方は <https://onebe.trustdelete.biz/>
 for FUJITSU をご利用の方は <https://onebe.trustdelete.biz/loginfj>
 ※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 ログインしたら、左メニューの[管理者]を選択し、運用に必要な情報を事前に確認します。

- 2.1 メールアドレスの変更が必要な場合はメールアドレスを入力し[設定保存]ボタンを押します。
このメールアドレスにコンピューターの登録時や消去完了時のメールが送信されます。
- 2.2 ログイン ID: 現在ログイン中の ID が表示されます。
- 2.3 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。
- 2.4 契約台数: お申込みいただいた台数が表示されます。
- 2.5 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。
- 2.6 終了日: ご契約の終了日が表示されます。
- 2.7 ご契約の更新および変更についての FAQ ページが表示されます。
- 2.8 アンインストールパスワードを入力し[設定保存]ボタンを押します。※初期段階では[0000]が登録されています。任意のパスワードに変更することをお勧めします。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にこのパスワードの入力が必要です。パスワードによってプログラムが不正にアンインストールされることを防ぎます。

※注意	<ul style="list-style-type: none"> ・アンインストールパスワードは、4～32 文字の半角英数文字がご利用できます。 ・アンインストールパスワードの初期値は[0000]です。 ・各項目を変更した場合は必ず[設定保存]ボタンを押してください。
-----	---

STEP2 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設定メニューについて説明します。設定メニューではクライアントプログラムの基本動作のほかに、どのフォルダー(ファイル)を消去するかを指定します。左メニューで[設定]を選択するとメニューバーが縦に開いて A01 から A04 が表示されます。A01 から A04 は同じ設定項目を備えており、それぞれ別の設定値を保存できます。つまり必要に応じて4パターンの設定をあらかじめ用意してコンピューターごとに使い分けることが可能となっています。

- | | |
|------|--|
| ※ヒント | <ul style="list-style-type: none"> ・デフォルトの設定は A01 です。つまりコンピューターのクライアントプログラムを登録すると自動で A01 が割り当てられます。そのあと任意の設定に変更は可能です。 ・A01 から A04 のすべてを設定する必要はありません。すべてのコンピューターを同じポリシーで運用する場合は A01 だけを設定してご利用ください。 |
|------|--|

ここではデフォルトの A01 の設定を説明します。A02 から A04 も設定方法は同じです。

管理メニュー

- ホーム HOME
- 設定 CONFIG
- A01
- A02
- A03
- A04
- S01
- 履歴 HISTORY
- グループ管理 GROUP ADMIN
- 管理者 ADMIN
- サポート SUPPORT
- ログアウト LOGOUT

設定 A01

設定登録・編集

設定名称: 営業部持ち出し用

設定保存

認証通信間隔 (消去命令の取得、不可視の確認、設定情報の更新)

認証間隔: 30分

プロキシの設定をロックする

位置情報を利用する

不可視設定

不可視機能を利用する

ネットワーク認証自動解除: ON OFF

解除ボタン有効時間: 2時間

タイマーロック設定

タイマーロックを利用する

タイマー: 1時間

SSIDを登録: 追加する

解除キー: trustd_unlock_A01_00.txt

自動消去設定

自動消去を利用する

1週間

一度も認証しないままこの時間を経過した場合、起動時に自動で消去を実行します

個別設定

設定を追加する

追加

消去	フォルダ名	消去方法	削除
<input checked="" type="checkbox"/>	デスクトップ	レベル1: 1回書込方式	
<input checked="" type="checkbox"/>	マイドキュメント	レベル: NSA方式	
<input checked="" type="checkbox"/>	メール	レベル: NSA方式	
<input checked="" type="checkbox"/>	ブラウザのお気に入り・キャッシュ・Cookie	レベル1: 1回書込方式	
<input checked="" type="checkbox"/>	Temp/tmpフォルダ	レベル1: 1回書込方式	
<input checked="" type="checkbox"/>	ごみ箱	レベル1: 1回書込方式	
<input type="checkbox"/>	Cドライブ	レベル1: 1回書込方式	
<input type="checkbox"/>	Dドライブ	レベル1: 1回書込方式	
<input checked="" type="checkbox"/>	BitLockerキー		

設定保存

©Copyright OneBe, Inc. All rights reserved

- ① [設定]をプルダウンして先頭の[A01]を選択します。
- ② [設定名称]:設定に 10 文字以内でオリジナルの名称を付けることができます。デフォルトは A01 です。
- ③ 認証通信間隔: 消去命令の取得、設定変更など各種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認証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。
- ④ プロキシ設定をロックする:チェックを入れるとクライアントプログラムの「ネットワーク設定」画面をロックしてコンピューター側での入力を無効にできます。ユーザーが勝手にプロキシ設定を変更して通信できなくなるのを防ぎます。
- ⑤ 位置情報を利用する:チェックを入れるとコンピューターの位置情報取得機能が有効になります。詳細は位置情報取得機能の項をご覧ください。
- ⑥ 不可視機能設定:詳細は不可視機能の項をご覧ください。
- ⑦ タイマーロック設定:詳細はタイマーロック機能の項をご覧ください。
- ⑧ 自動消去設定:詳細は自動消去機能の項をご覧ください。
- ⑨ 固定設定:消去する領域を決められた範囲の中から選択して指定することができます。固定設定の各項目の領域は次の通りです。

- ◆ **デスクトップ:** すべてのユーザーのデスクトップ上のファイル/フォルダー
- ◆ **マイドキュメント:** すべてのユーザーの Document フォルダー
- ◆ **メール:** Windows10 および Windows8/8.1 の Windows ストアアプリのメール、Windows Mail、Windows Live Mail、Outlook、Outlook Express のメール本文およびアドレス帳データ
- ◆ **ブラウザのお気に入り・キャッシュ・Cookie:** すべてのユーザーの Internet Explorer のお気に入り、インターネット一時ファイル、Cookie、履歴、保存されたパスワード、Web フォームの情報
- ◆ **Temp/tmp フォルダー:** すべてのユーザーの AppData¥Local¥Temp フォルダー
- ◆ **ごみ箱:** ごみ箱内のファイル
- ◆ **Cドライブ:** Cドライブ上のデータ(※一部のシステムファイルを除く)
- ◆ **Dドライブ:** Dドライブ上のデータ
- ◆ **BitLocker キー:** BitLocker キーを初期化して Windows を起動不可の状態にします。(BitLockerキーの消去を参照)

※注意	Outlook は Outlook 2010, 2013, 2016 に対応しています。 PST メールと Exchange メール(OST)の双方に対応しています。
※注意	Windows10 および Windows8/8.1 のストアアプリのメールは Exchange メールのみ対応しています。また消去を実行するとメールアプリケーションおよび関連するいくつかのアプリケーションがアンインストールされます。
※注意	Outlook、Outlook Express、Windows Live Mail はログオン中のユーザーのデータが対象となります。
※注意	メール本文の消去を実行するとメールデータ以外にアカウント情報が消去されることがあります。Exchange をご利用の場合、Exchange のアカウントもなくなります。
※注意	「ブラウザのお気に入り・キャッシュ・Cookie」消去機能はバージョン 8.0.49 以降でご使用いただけます。バージョン 8.0.29 以前をご使用の場合には「ブラウザのお気に入り」消去機能のみ働きます。

※注意	「ブラウザのお気に入り・キャッシュ・Cookie」消去機能はログオフ状態では、履歴の消去、Web フォームの消去、パスワードの消去は働きません。
※注意	「ブラウザのお気に入り・キャッシュ・Cookie」消去機能は Microsoft Edge には対応していません。
※注意	Temp フォルダは C:¥Users¥ユーザー名¥AppData¥Local¥Temp が対象です。 C:¥Wnodws¥Temp は対象にはなりません。
※注意	ごみ箱内のファイル消去はバージョン 8.0.49 以降でご使用いただけます。バージョン 8.0.29 以前をご使用の場合には働きません。
※注意	CドライブまたはDドライブを消去指定してもWindowsの起動や本プログラムの実行に必要なファイルは消去されません。 消去の対象外となるもの:Windows フォルダ、OSの起動に必要なフォルダ、システムファイルフォルダ、本プログラムインストールフォルダ等

- ⑩ 個別設定:固定設定以外の任意のファイル/フォルダを消去する場合に利用します。最大50項目までオリジナルの設定を作成することができます。
消去したい任意のフォルダのディレクトリをドライブ名からフルパスで入力し、左のチェックボックスにチェックを入れてください。
個別のファイルを指定する場合はそのファイルのフルパスを指定してください。このときファイル名に必ず拡張子も忘れずに指定してください。

例)C:¥Users¥TANAKA¥Desktop¥1 月売上表.xls

※注意	<ul style="list-style-type: none"> 個別設定枠の右上の[追加]ボタンをクリックすると空白の行が下に追加されます。 ファイルやフォルダのパスを入力するときはファイル名、¥マークやスペースなど間違いのないように確認してください。 パスは最大で255文字まで入力可能です。
-----	---

- ⑪ 消去方法の選択:
- ◆ レベル1(1回書き込み):レベル9と比較して消去能力はやや劣りますが、消去スピードが約60%と速いため、大容量データを消去する場合におすすめです。0×1回書き込み。
 - ◆ レベル9(NSA方式):消去能力が高いですが時間がかかるため、重要かつ容量の小さいデータを消去するのにおすすめです。乱数書き込み×2回、0×1回、合計3回書き込み。

※ヒント	消去の対象フォルダはコンピューターを盗難・紛失した場合、消去命令を発行する直前に指定または変更することも可能です。
※注意	対象フォルダ内にファイルが多く存在する場合には、コンピューター側ですべてを消去するまでに長い時間を必要とします。盗難・紛失時に、効果的にデータを消去するためには、はじめに重要なデータのみを選択して消去対象にすることをお勧めします。CドライブやDドライブを消去する場合はご注意ください。

- ⑫ 以上すべての設定が完了したら、画面の右側にある[設定保存]ボタンを必ず押してください。ボタンは画面の上下にあります、どちらか片方を押すだけで保存されます。

※注意	[設定保存]ボタンを押すまで設定項目は保存されません。
-----	-----------------------------

STEP3 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[サポート]ボタンをクリックします。別ウインドウでサポートページが開いたら、メニューから「プログラムのダウンロード」をクリックしてプログラムをコンピュータに保存します。ダウンロードしたインストールプログラム(TDInst.exe)をダブルクリックしてインストールしてください。
※インストールの詳細は**クライアントマニュアル**をご覧ください。
2. インストールが終了したら以下の手順で必ず利用登録を実行してください。
※利用登録にはあらかじめ8桁のシリアル番号をご用意ください。シリアル番号は[ユーザー登録完了のご案内メール]に記載のほか、[管理者]メニューでもご確認いただくことができます。
シリアル番号は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。利用登録を必ず行ってください。
-----	--

STEP4 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[ホーム]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]に適切な番号(A01 から A04)が割り当てられているか確認し、必要に応じてプルダウンから設定番号を選択してください。変更する場合は必ず[設定保存]を押してください。

管理メニュー

- ホーム HOME
- 設定 CONFIG
- 履歴 HISTORY
- グループ管理 GROUP ADMIN
- 管理者 ADMIN
- サポート SUPPORT
- ログアウト LOGOUT

ホーム

コンピューター検索 ▲

接続日時検索 ▲

CSV編集
インポート エクスポート

表示をリセット

最大表示数 25件

登録解除 設定保存

すべて選択

タイプ	設定	コンピューター名	利用者	発動条件	ステータス	備考	最終接続日時	選択
	A02	PC-001	佐藤				2015-09-07 17:46:05	<input type="checkbox"/>
	A01	PC-002	田中		10月末まで出張中		2015-09-07 17:45:51	<input type="checkbox"/>
	A02	PC-003	中村				2015-09-07 17:45:36	<input type="checkbox"/>
	A01	PC-004	鈴木				2015-09-07 17:45:21	<input type="checkbox"/>
	A02	PC-005	加藤				2015-09-07 17:45:02	<input type="checkbox"/>

登録解除 設定保存

[5 (1 - 5)] 1

©Copyright OneBe, Inc. All rights reserved

ホーム

リモートロック 消去命令

詳細情報

設定: ① 設定A01

コンピューター名: ② PC-006

解除パスワード: ③ 0000

利用者: ④ KATO

所属グループ: ⑤ 営業部

備考: ⑥

電話番号:

機種品番: ⑦ CF-SX3EFRTS

製造番号: ⑧ 3IKSA00924

プログラムVer: ⑨ Ver. 8.0.68.0

登録日時: ⑩ 2015-08-13 17:40:55

最終履歴: ⑪ 2015-08-18 14:20:14 消去命令 キャンセル

ロック状態: ⑫ アンロック

タイマーロック解除: ⑬

以前の履歴を見る: ⑭ ⑮ 位置情報を表示

⑯ 設定保存 キャンセル

- ① 設定: このコンピューターに割り当てられている設定番号と設定名が表示されます。
- ② コンピューター名: コンピューターの利用登録時に自動で取得します。
- ③ 解除パスワード: 不可視を一時的に解除するためのパスワードです。4 から 32 文字の英数字を設定できます。初期設定では[0000]が設定されています。
- ④ 利用者: このコンピューターの利用者の氏名を入力してください。(空白でも支障ありません)
- ⑤ 所属グループ: このコンピューターを任意のグループに割り当てることで部署単位での管理を可能にします。部署別の管理が不要な場合は空白のままでも支障ありません。詳しくはグループ管理の項をご覧ください。
- ⑥ 備考: 任意の補足情報を最大 500 文字まで入力できます。(空白のままでも支障ありません)
- ⑦ 機種品番: コンピューターの機種品番を表示します。
- ⑧ 製造番号: コンピューターの製造番号を表示します。
- ⑨ プログラム Ver: クライアントプログラムのバージョンを表示します。
- ⑩ 登録日時: このコンピューターが利用登録した日時を表示します。
- ⑪ 最終履歴: このコンピューターで操作した最新の命令および発行日時を表示します。
- ⑫ ロック状態: コンピューターがロックされているかどうか状態を表示します。
- ⑬ タイマーロック解除: タイマーロックを遠隔操作で解除する際に使用します。
- ⑭ 以前の履歴を見る: このコンピューターに対する操作履歴を一覧で表示します。
- ⑮ 位置情報を表示: このコンピューターの位置情報を別ウィンドウで表示します。詳しくは位置情報機能の項をご覧ください。
- ⑯ 設定保存: 以上の入力設定が完了したら、必ず[設定保存]ボタンを押してください。

※注意	[設定保存]ボタンを押すまで設定はシステムに反映されません。
※ヒント	[キャンセル]ボタンを押すとホーム画面に戻ります。
※ヒント	利用者氏名や備考欄の情報を変更する場合は現在の入力をいったん消去してから新たに値を上書き入力してください。

4. 上記の設定が完了し、[設定保存]を押したら、左メニューの[ホーム]をクリックします。
[A01]のプルダウンの枠がピンク色に変わっています。設定のプルダウンがピンクになっているときは設定の更新以降にそのコンピューターが管理サーバーに認証していない状態を表しています。コンピューターが管理サーバーに認証して最新の設定情報を取得すると表示がピンクから白に戻ります。

5. [設定]メニューで A01 以外 (A02 から A04) の設定を作成して、それをコンピューターに適用する場合はプルダウンから任意の設定番号を選択してから[設定保存]をクリックします。

※注意	[設定保存]ボタンを押すまで設定はシステムに反映されません。
-----	--------------------------------

※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する必要があります。管理サーバーで設定を変更するたび、クライアントプログラムの[接続]ボタンを押して手動で認証を実行して最新の設定を取り込むことをお勧めします。

STEP 5 利用者への告知

以上で TRUST DELETE Biz 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 STEP 2 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(3 項)やタイマーロック機能(7 項)を活用する

下記の URL では、利用者に向けた注意事項をまとめた資料を公開しています。貴社にてご利用中の機能や、緊急時の報告窓口などを編集したうえで利用者に配布できるよう、PPT 形式で公開していますので、利用者向けの告知にご活用ください。

利用者向け配布資料ダウンロード URL <https://www.onebe.co.jp/handout/>



TRUSTDELETE Biz

パソコンの紛失・盗難時の報告

● 持ち出したパソコンを紛失した！
● パソコンが盗難に遭った！

パソコンを紛失しました!!

情報の漏えいを防ぐために、盗難・紛失かも知れないと気付いたら**直ちに、所定の窓口や上へ報告**してください。
※紛失したかどうか不明な場合も、無名が不明でも報告してください。

報告先

- 電話： XXXX-XXXX-XXXX
- 夜間： XXXX-XXXX-XXXX
- メール： XXXX@XXXX.XXX.XX
- 会社名： OOOO会社

報告によって、登録担当者や速やかにパソコンの消去を依頼したり、遠隔操作により情報漏えいを防止でき、バックアップが完了します。

※パソコンのトラブルにだけ対応するのではなく、様々な場面で対応します。

リモートワーク・在宅勤務時

注意事項

パソコンを社外に持ち出すことは、利便性が上がる半面、情報が漏洩するリスクも上がるため、次の注意が必要です。

- パソコンの持ち出しは必要時のみにする。
- 外出先で不要な機密情報は、保存しない、持ち出さない。

当社のパソコンは、盗難・紛失時に遠隔地からデータを消去して、情報漏えいを防止する対策が施されています。

ワンビ株式会社「TRUST DELETE Biz」を利用し、次の機能をパソコンを情報漏えいから守ります。

- ✓ **パソコンの情報漏えい防止**
業務に利用しないパソコンによる、紛失したパソコンを捜すことができず、
✓ **紛失しても情報漏えい防止**
リモートワークやデータの消去に成功し、紛失したと気付いたら、すぐに遠隔操作に連絡していただきます。
- ✓ **盗難・ネットに接続し続けられデータを自動消去**
パソコンを盗難する際は、ネットにつながりながら消去していただき、
 チェックされている対策を実施しています。

TRUSTDELETE Biz

TRUSTDELETE Biz のセキュリティ機能

パソコンが一時的にインターネットに接続され、管理サーバとの通信がない場合、以下の機能が作動します。

- ✓ **ロック機能が作動しパソコン操作不能となり、下記のような画面が表示されます。**
Windows を起動してすぐインターネットに接続し、5 分以内で管理サーバへの接続がなければ、ロックはできません。
ロック機能が作動し、下記の画面でロック画面が表示され、報告窓口へ連絡して待機して下され。
- ✓ **パソコン内のデータが自動消去されます。**
Windows を起動してすぐインターネットに接続し、5 分以内で管理サーバへの接続がなければ、自動消去はできません。
 チェックされている対策を実施しています。

もし、パソコンを紛失した場合どうなるか？

パソコンはどこでも使用できるため便利な反面、様々な場面で情報漏えいのリスクがあります。情報漏えい事故の多くが、**紛失**もしくは**盗難**より起きています。パソコンを失った際には迅速な対応が求められ、内容によっては**組織に大きな影響**を及ぼすおそれがあります。

盗難防止
盗難防止
盗難防止

盗難防止
盗難防止
盗難防止

盗難防止
盗難防止
盗難防止

盗難防止
盗難防止
盗難防止

順位	種類	割合
1位	紛失・盗難	45.0%
2位	誤表示・誤配信	20.0%
3位	ウイルス感染・不正アクセス	13.6%
4位	盗難	11.6%

参考：東京工科大学「上場企業の個人情報漏えい・紛失事故調査」

2. コンピューター紛失時の消去命令の発行

万が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。

STEP1 管理サーバーにログイン

ID とパスワードで管理サーバーログインします。

STEP2 対象設定の確認

紛失したコンピューターをコンピューター名や利用者氏名の情報をもとに特定します。

命令発行の前に消去設定を変更する場合はプルダウンから希望の設定を選んで[設定保存]ボタンを押してください。

The screenshot shows the 'ホーム' (Home) page of the management interface. A table lists computer details. The row for 'PC-006' is highlighted with a red box, and a blue arrow points to it with the text 'Click!'.

タイプ	設定	コンピューター名	利用者	ステータス	所属グループ	備考	最終接続日時	選択
	A02	PC-001	佐藤		開発部		2013-09-22 08:11:09	<input type="checkbox"/>
	A01	PC-002	田中		営業部	10月末まで出張中	2013-09-22 08:10:39	<input type="checkbox"/>
	A02	PC-003	中村		開発部		2013-09-22 08:11:09	<input type="checkbox"/>
	A01	PC-004	鈴木		営業部		2013-09-22 08:10:39	<input type="checkbox"/>
	A02	PC-005	加藤		開発部		2013-09-22 08:11:09	<input type="checkbox"/>
	A01	PC-006	KATO		営業部		2013-09-22 08:10:39	<input type="checkbox"/>

STEP3 消去命令を発行

該当のコンピューター名をクリックして詳細情報画面を開きます。画面右上の[消去命令]ボタンを押して命令発行の確認画面が表示されたら[OK]をクリックします。

The screenshot shows the detailed information page for computer PC-006. The '消去命令' (Delete Command) button is highlighted with a red box and a blue arrow pointing to it with the text 'Click!'.

設定: [設定A01] [設定保存] [キャンセル]

コンピューター名: PC-006

解除パスワード: [0000]

利用者: [KATO]

所属グループ: [営業部]

備考: []

電話番号: []

機種品番: CF-SX3EFRTS

製造番号: 31KSA00924

プログラムVer: Ver. 8.0.68.0

登録日時: 2015-08-13 17:40:55

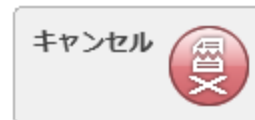
最終履歴: 2015-08-18 14:20:14 消去命令 キャンセル

ロック状態: アンロック

タイマーロック解除: []

以前の履歴を見る [] 位置情報を表示 []

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



これで消去命令の発行は完了です。ホーム画面に戻るとステータスが[命令発行]と表示されます。あとはコンピューターがネットワークに接続して消去命令を受け取るのを待ちます。

コンピューターが消去命令を取得すると[キャンセル]ボタンが[消去中]に変わり赤く点滅します。
 ※表示が[消去中]になると命令の取り消しはできません。



このあとコンピューター側で消去が完了すると[消去中]のボタンが元の[消去命令]に戻ります。ホームや履歴メニューのステータスに[消去完了]と表示されます。



※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に接続するまでは実際には消去は開始されません。
※ヒント	紛失したコンピューターが起動してネットワークに接続する頻度が高いほど消去命令が届きやすく、速やかに消去が始まる可能性が高くなります。画面上の[最終接続日時]を参考にしてコンピューターが定期的に接続しているかどうか推測できます。接続頻度が低いコンピューターは消去命令を受け取れないこともあります。
※ヒント	消去が完了してもコンピューターがネットワークに接続するまで結果は不明です。従って、実際には消去が終わっていても消去中の表示のままになることがあります。
※注意	消去命令を発行中または消去中のコンピューターは設定変更や登録解除ができません。設定変更や登録解除が必要な場合は、いったん消去命令を取り消すか、消去が完了するまでお待ちください。

消去命令をキャンセルする

ホーム画面でコンピューター名をクリックして詳細情報を表示します。右上の[キャンセル]ボタンをクリックします。確認画面のウィンドウが表示されるので[OK]をクリックします。命令をキャンセルするとボタンは[消去命令]に戻ります。

※注意	コンピューターがいったん消去命令を取得して、表示が[消去中]になると消去を停止することはできません。
-----	--

3. 自動消去機能

時限爆弾のように特定の条件下で一定時間が経過すると、管理サーバーからの消去命令がなくても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。紛失したコンピューターがネットワークに接続できない状況でもクライアントプログラム側の判断で消去を実行可能です。

自動消去の実行条件

あらかじめ管理サーバーで自動消去実行までの時間を選択します。選択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、自動消去がスタートします。電源 OFF の間や休止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て認証した場合、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せん。

設定方法

設定メニューを開きます。

自動消去を利用する： ボックスにチェックを入れると自動消去機能が有効になります。

設定時間： 自動消去開始までのタイマー時間を選択します。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自動消去が実行されます。

24 時間、48 時間、72 時間、1 週間、2 週間、3 週間、4 週間、60 日、90 日間から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、必ず画面右上の[設定保存]ボタンを押してください。

<p>不可視設定</p> <p><input checked="" type="checkbox"/> 不可視機能を利用する ▲</p> <p>ネットワーク認証自動解除: <input checked="" type="radio"/> ON <input type="radio"/> OFF</p> <p>解除ボタン有効時間: 2時間 ▼</p>	<p>タイマーロック設定</p> <p><input checked="" type="checkbox"/> タイマーロックを利用する</p> <p>タイマー: 1時間 ▼ SSIDを登録: <input type="button" value="追加する"/></p> <p>解除キー ▲:</p> <p><input type="button" value="ダウンロード"/> trustd_unlock_A01_00.txt <input type="button" value="キーの更新"/></p>
<p>自動消去設定</p> <p><input checked="" type="checkbox"/> 自動消去を利用する ▲</p> <p>1週間 ▼ 一度も認証しないままこの時間を経過した場合、起動時に自動で消去を実行します</p>	

どのフォルダーを消去するか

自動消去の実行時に消去されるフォルダーは消去対象に設定されたフォルダーと共通です。ただし自動消去は管理サーバーと接続しない条件下で作動するため、消去対象の設定があらかじめクライアントプログラムに取り込まれている必要があります。消去命令発行時と異なり、直前に設定した消去対象が自動消去に反映される可能性が少ないので注意してください。

重要事項（必ずお読みください）

- ◆ 不測の事態により誤って自動消去が開始することを防ぐために、コンピューターの起動から5分間の猶予期間を設けています。そのため自動消去の実行日時になっても、コンピューターの起動から5分以内にネットワークに接続してサーバーと認証すると、自動消去はリセットされます。
- ◆ タイマー時間を過ぎて実行条件が満たされると、OSが起動したタイミングで(5分以内に認証しなければ)自動消去は実行されます。本機能を解除するには自動消去タイマーが指定時間に達する前にコンピューターをサーバーと接続して認証してください。万一、不測の事態で指定時間より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した状態でコンピューターを起動して、起動後5分以内にサーバーと認証してください。
- ◆ タイマー時間を過ぎるとコンピューターの起動、スリープや休止からの復帰のタイミングで自動消去が実行されます。
- ◆ コンピューターの時刻(OSまたはBIOSのシステムクロック)を12時間以上戻した場合、時刻違反を検出して自動消去を実行します。くれぐれもご注意ください。
- ◆ 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勧めします。
- ◆ 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る状態では指定した時間が経過した時点で自動消去が実行されますのでご注意ください。
- ◆ 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一定時間使用できなくなる可能性を考慮して余裕のあるタイマー時間を選択してください。
- ◆ 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自動消去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、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、ご利用になるようご注意ください。

4. BitLocker キーの消去

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 と併用することで、リモートでコンピューターを起動不可能な状態にすることができます。本機能は 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。

動作条件

- BitLocker ドライブ暗号化を有効にしていること
- コンピューターに TPM が搭載され、TPM を暗号キーとして使用していること

設定方法

STEP1 BitLocker を有効にする

BitLocker の設定方法はコンピューターまたは Windows のマニュアルを参照してください。

※注意	BitLocker の設定時に回復キーを必ず作成し大事に保管してください。一度 BitLocker 消去を実行すると回復キーがないとそのコンピューターを起動できません。
-----	--

STEP2 BitLocker キーを消去対象にする

設定メニューでお使いになる設定 (A01 から A04) を選択し、[BitLocker キー] の消去にチェックマークを入れたのち、必ず[設定保存]ボタンをクリックしてください。

STEP3 消去命令を発行する

通常の消去と同じように消去命令を発行してください。通常の消去(ファイル保存場所を指定する方法)と同時に利用することができます。マイドキュメントやメールの消去と併せて BitLocker キーを消去することで、暗号化済みのディスクを保護することが可能です。

クライアントプログラムは BitLocker キーを消去した後、自動でコンピューターをシャットダウンします。シャットダウン直前にインターネット接続があれば消去完了を管理サーバーに通知してからシャットダウンします。その後、コンピューターの電源を投入しても Windows は起動しません。次回から起動時に[Windows BitLocker ドライブ暗号化の回復キーの入力]画面が表示され、回復キーを入力しない限りコンピューターが起動できなくなります。コンピューターを回復キーで起動して認証に成功すると消去完了扱いになります。

※注意	BitLocker キーのみを消去した場合、ステータスレポートの消去ファイル数は[0]と表示されます。
※ヒント	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。
※注意	トラストデリートでは、「BitLocker ドライブ暗号化」に対応しています。「デバイスの暗号化(Windows8.1 からの機能)」には対応していません。

5. 不可視機能

不可視機能とは

紛失したコンピューターがインターネットに接続していない環境では、消去命令を発行しても命令を取得することができません。不可視機能を利用することでコンピューターがオフラインの場合でもデータを保護することが可能になります。デスクトップやマイドキュメントなど通常の操作で使用する領域内のデータを瞬時に秘匿することでデータを不正アクセスから守ります。不可視化されたデータは見つけることはできませんが、ディスク上に残っているので、瞬時に元に戻すことが可能です。不可視機能は管理サーバーで有効・無効を選択できます。

どのフォルダーが不可視になるのか

ライブラリー配下のデータが不可視の対象となります。これにはデスクトップやマイドキュメント、マイピクチャー、マイビデオ、ダウンロードなどのほか主要メーカーのメールデータ等も含まれません。不可視の対象領域を選択設定することはできません。

不可視機能の実行タイミング

インターネット接続がなく、クライアントプログラムが管理サーバーと認証に失敗すると、即座に不可視機能が働きます。

- ✓ コンピューターの起動直後やスリープや休止からの復帰時にインターネット接続できない場合
- ✓ 定期的な認証通信(ポーリング)時にインターネット接続できない場合

不可視機能を有効にするには

設定メニューの[不可視機能を利用する]にチェックを入れて[設定保存]を押してください。

不可視の解除その1: ネットワーク認証

設定メニューにある[ネットワーク認証自動解除]を ON にすると、不可視が作動したあと、コンピューターがインターネットに接続すると自動で不可視を解除できます。

OFF を選択するとコンピューターがオンラインになっても解除されません。

不可視の解除その2: 手動解除

移動中の交通機関の中などインターネットが使えない環境では1のネットワーク自動解除が利用できません。しかしオフライン環境でも手動で不可視を一時的に解除することが可能です。

[解除ボタン有効時間]のプルダウンから任意の時間を選択してください。

クライアントプログラムの[不可視解除]ボタンを使うと、プルダウンから選択した時間に限り、不可視になったデータを一時的に元通りに表示することができます。

[解除ボタン有効時間]は無効、30分、1時間、2時間から選択することができます。

手動による一時解除のあと、解除ボタン有効時間が経過すると再びデータが不可視になります。

ここで[無効]を選択すると[不可視解除]ボタンが利用できなくなり、手動解除が使えません。

※コンピューターを手動解除する方法はクライアントマニュアルを参照してください。

6. リモートロック機能

リモートロック機能は遠隔操作でコンピューターのマウスやキーボード、タッチパッドやタッチパネル、デジタイザー等の入力デバイスを無効化してコンピューターを一時的に操作不能にする機能です。

STEP1 管理サーバーにログイン

ID とパスワードで管理サーバーログインします。

STEP2 対象設定の確認

紛失したコンピューターをコンピューター名や利用者氏名の情報をもとに特定します。

The screenshot shows the 'ホーム' (Home) page of the management interface. A table lists computer details. The row for 'PC-006' is highlighted with a red box, and a blue arrow points to it with the text 'Click!'.

タイプ	設定	コンピューター名	利用者	ステータス	所属グループ	備考	最終接続日時	選択
	A02	PC-001	佐藤		開発部		2013-09-22 08:11:09	<input type="checkbox"/>
	A01	PC-002	田中		営業部	10月末まで出張中	2013-09-22 08:10:39	<input type="checkbox"/>
	A02	PC-003	中村		開発部		2013-09-22 08:11:09	<input type="checkbox"/>
	A01	PC-004	鈴木		営業部		2013-09-22 08:10:39	<input type="checkbox"/>
	A02	PC-005	加藤		開発部		2013-09-22 08:11:09	<input type="checkbox"/>
	A01	PC-006	KATO		営業部		2013-09-22 08:10:39	<input type="checkbox"/>

STEP3 リモートロック命令を発行

該当のコンピューター名をクリックして詳細情報画面を開きます。画面右上の[リモートロック]ボタンを押して命令発行の確認画面が表示されたら[OK]をクリックします。

The screenshot shows the detailed information page for computer PC-006. The 'リモートロック' button is highlighted with a red box, and a blue arrow points to it with the text 'Click!'.

設定: 設定A01

コンピューター名: PC-006

解除パスワード: 0000

利用者: KATO

所属グループ: 営業部

備考:

電話番号:

機種品番: CF-SX3EFRTS

製造番号: 3IKSA00924

プログラムVer: Ver. 8.0.68.0

登録日時: 2015-08-13 17:40:55

最終履歴: 2015-08-18 14:20:14 消去命令 キャンセル

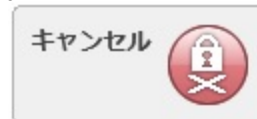
ロック状態: アンロック

タイマーロック解除:

以前の履歴を見る:

位置情報を表示:

リモートロック命令が発行されると、ボタンが[キャンセル]に変わります。
※この段階ではロック命令を取り消すことができます。



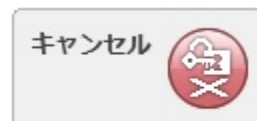
これでリモートロック命令の発行は完了です。ホーム画面に戻るとステータスが[命令発行]と表示されます。あとはコンピューターがネットワークに接続して命令を受け取るのを待ちます。

コンピューターがリモートロック命令を取得すると[キャンセル]ボタンが[リモートアンロック]に変わります。



STEP4 リモートロックの解除方法

リモートロックされたコンピューターをロック解除するにはアンロック命令を発行します。[リモートアンロック]ボタンを押して確認画面が表示されたら[OK]をクリックします。
※この段階ではアンロック命令を取り消すことができます。



コンピューターがネットワークに接続してアンロック命令を受信するとボタン表示が[リモートロック]に戻ります。



※注意	リモートロックやリモートアンロック命令を発行してもコンピューターが管理サーバーに接続するまでは実際にはロックまたはアンロックされません。
※注意	消去命令の発行中は一時的にリモートロックまたはリモートアンロックのボタンは操作できなくなります。消去命令をキャンセルするか消去が完了するとロック／アンロックのボタンが有効になります。ロックやアンロックが先に発動していても消去命令を発行すれば消去命令が優先的に作動します。
※ヒント	リモートロックとリモートアンロックはそれぞれ交互に利用可能となります。
※注意	リモートロック/リモートアンロックはバージョン 8.0.71 以降でご使用いただけます。バージョン 8.0.60 以前をご使用の場合には実行することはできません。
※注意	リモートロック命令を発行中はタイマーロックの解除を利用できません。

オフライン状態でリモートロックを一時的に解除する方法

リモートロックされたコンピューターがネットワークに接続できない状態でもロック解除キーを用いて一時的にアンロックすることが可能です。

設定メニューの[タイマーロック設定] で解除キーの[ダウンロード]ボタンをクリックしてキーファイ

ルを保存します。保存したキーファイルを USB メモリに保存してください。この時 USB メモリ内のルートに直にファイルを保存します。メモリ内のフォルダーに保存しないでください。
ロック中のコンピューターに解除キーファイルの入った USB メモリを挿すと 60 分間ロックが解除されます。解除から 60 分経過すると自動でロックされますが解除キーを挿すと再び 60 分間ロック解除できます。

※注意	解除キーによるロック解除は時間制限のある一時的なものであり、ロック状態を完全にリセットするものではありません。リモートアンロック命令が受信できない状況で一時的にコンピューターを使用するためにご利用ください。 恒久的にアンロックするにはコンピューターをネットワークに接続してリモートアンロック命令を実行してください。
※ヒント	解除キーの詳細はタイマーロックの項を参照してください。
※注意	解除キーによるロック一時解除中はタイマーロックは発生しません。
※注意	解除キーによるロック一時解除中に、管理コンソールで設定保存を行った場合には、コンピューターが認証を行った時に 60 分を経過していなくても再ロックされます。

7. タイマーロック機能

タイマーロック機能は命令操作なしにタイマーによってコンピューターの入力デバイスを無効化してコンピューターを一時的に操作不能にする機能です。

ロックの実行条件

ロック機能はタイマーによって動作します。ロック実行までのタイマー時間は管理サーバーで設定します。タイマー時間内にコンピューターがインターネットに接続して認証に成功しなければ、コンピューターはロックされます。電源 OFF の間やスリープ、休止状態の経過時間もカウントされません。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て認証に成功した場合、その時点でタイマーがリセットされ、計測がゼロから再開されます。

タイマー時間を過ぎた後にコンピューターを起動する場合、起動から 5 分以内にインターネットに接続して認証に成功させることでロックを回避できます。

設定方法

設定メニューで[タイマーロックを利用する]にチェックを入れます。

すぐ下の[タイマー]のプルダウンから任意の時間を選択します。

ロックの[タイマー]は、30 分、1 時間、2 時間、6 時間、12 時間、24 時間、48 時間、72 時間、1 週間、2 週間から選択することができます。

※以上の設定を行った後、必ず画面右上の[設定保存]ボタンを押してください。

※注意	<ul style="list-style-type: none"> ・コンピューターが管理サーバーに認証するたびにタイマーはリセットされ、ゼロから再開します。 ・下記に記載のいずれかの解除方法でロックを解除した場合はコンピューターがオンライン/オフラインに限らずタイマーはリセットされます。 ・リモートロック命令によってすでにロック状態のコンピューターは指定のタイマー時間が経過してもタイマーロックは作動しません。
-----	---

解除方法

解除の方法は次の 3 通りがあります。

◆ 解除方法1 解除キー

ロック中のコンピューターに解除キーファイルの入った USB メモリを挿すことでロックを解除する仕組みです。

設定メニューの[タイマーロック設定]で解除キーの[ダウンロード]ボタンをクリックしてキーファイルを保存します。保存したキーファイルを USB メモリに保存してください。この時 USB メモリ内のルートに直にファイルを保存します。メモリ内のフォルダーに保存しないでください。

解除キーを更新するには？

一度使用した解除キーが出回ると、誰でも安易にロック解除できるようになる危険性があり

ます。これを防ぐため、次の方法で解除キーを変更することが可能です。

1. 画面に表示されている現在のキーファイル名をメモします。
2. 現在のキーファイルを保存していない場合は、あらためてキーファイルを保存します。
3. 画面内の[キーの更新]ボタンをクリックします。確認画面が表示されたら[OK]を押します。ボタン左横のキー番号の末尾が 1 番アップするのを確認してください。
4. [ダウンロード]ボタンをクリックして新しいキーファイルを保存します。
5. 新しいキーファイルを USB メモリに保存します。(古いキーと同じ USB メモリに保存可能です)
6. 上記の操作のあと、コンピューターが管理サーバーに認証したタイミングでコンピューター側の解除キーも更新されます。その後は新しいキーが有効になります。

※重要※

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認証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。従って、キーを更新する前に常に現行のキーを忘れずに保存してください。

※注意	<ul style="list-style-type: none"> ・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。 ・キーを更新する際は常に歴代のキーファイルを保存しておくことをお勧めします。 ・キーファイルは A01 から A04 まで設定ごとに異なります。 ・同じ設定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。つまり A01 が設定されたコンピューターが 10 台ある場合、これら 10 台は同じ解除キーでロックが解除できることとなります。 ・リモートロックと異なり、タイマーロックでは解除キーを使うことで完全にロック解除されます。リモートロックでは解除キーによるアンロックは 60 分の制限時間つきです。
-----	--

◆ 解除方法 2 無線 LAN 検出解除

ロックされたコンピューターがあらかじめ指定した無線 LAN のアクセスポイントに接続して SSID を検出した場合に自動でロック解除する仕組みです。例えばオフィスのアクセスポイントの SSID を登録しておく、ロックされたコンピューターがオフィスに戻って無線 LAN を検出すると自動でロック解除が働きます。

設定メニューの SSID を登録の右横の[追加する]ボタンをクリックします。
登録画面が開いたら希望の SSID を入力して[登録]ボタンをクリックします。
SSID は最高 10 個まで登録できます。

この解除方法はロックしたコンピューターが Wi-Fi オンの状態で登録済みの SSID を検出する必要があります。登録した SSID に接続する必要はございません。無線 LAN ルーターに有線接続しても解除されません。

登録済みの SSID を削除する場合は[追加する]ボタンを押して、画面を表示して入力済みの SSID を削除してから[登録]ボタンを押してください。

◆ 解除方法 3 遠隔操作によるロック解除

ロックされたコンピューターにインターネット経由で解除命令を発行することでロック解除する

ことができます。指定の無線 LAN アクセスポイントや USB 解除キーが使用できない環境で有効ですが、解除対象のコンピューターがインターネットに接続する必要があります。

ホーム画面でロック解除したいコンピューターを選択してコンピューター名をクリックして詳細画面を表示します。

画面下部の[タイマーロック解除]のボタンをクリックします。タイマーロック解除実行の確認画面が表示されたら[OK]をクリックします。

このあとコンピューターが管理サーバーに接続してきたタイミングで解除命令が伝達されロック解除されます。

The screenshot shows the 'Home' page of the TRUST DELETE Biz management interface. At the top, there are navigation buttons for 'Home', 'Remote Lock', and 'Clear Command'. Below the navigation bar, there is a '詳細情報' (Detailed Information) section for a specific computer. The information includes:

- 設定: 設定A01
- コンピューター名: PC-006
- 解除パスワード: 0000
- 利用者: KATO
- 所属グループ: 営業部
- 備考: (empty text area)
- 電話番号: (empty)
- 機種品番: CF-SX3EFRTS
- 製造番号: 3IKSA00924
- プログラムVer: Ver. 8.0.68.0
- 登録日時: 2015-08-13 17:40:55
- 最終履歴: 2015-08-18 14:20:14 消去命令 キャンセル
- ロック状態: アンロック
- タイマーロック解除: (button highlighted in red)

At the bottom of the information panel, there are two buttons: '以前の履歴を見る' (View previous history) and '位置情報を表示' (Display location information).

※注意	タイマーロック解除ボタンを押してもコンピューターが管理サーバーと接続するまではロック解除は実行されません。
※注意	タイマーロック解除機能を実行しても、ステータス表示、履歴の作成を行いません。
※注意	タイマーロック解除機能はバージョン 8.0.71 以降でご使用いただけます。バージョン 8.0.60 以前をご使用の場合には実行することはできません。
※注意	タイマーロック解除機能を実行中はリモートロック命令を利用できません。
※ヒント	タイマーロック解除機能はロック状態にかかわらず実行可能です。コンピューターがデバイスロックされていない状態で、受信された場合には何もおきません。

8. 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[履歴]メニューでは各コンピューターの状況を確認できます。

タイプ	コンピューター名	実行日時	発動条件	ステータス	選択
	PC-001	2015-08-18 14:19:43	消去命令	キャンセル	<input type="checkbox"/>
	PC-002	2015-08-18 14:19:24	自動消去	完了	<input type="checkbox"/>
	PC-001	2015-08-13 19:00:18	消去命令	完了	<input type="checkbox"/>
	PC-003	2015-08-13 19:00:11	リモートアンロック	完了	<input type="checkbox"/>
	PC-003	2015-08-13 18:59:10	リモートロック	完了	<input type="checkbox"/>

発動条件とステータス

命令種類	発動条件	ステータス		
		発行直後	命令受信後	命令実行後
消去命令	消去命令	命令発行	実行中	完了
自動消去	自動消去	-	-	完了
リモートロック	リモートロック	命令発行	実行中※	完了
リモートアンロック	リモートアンロック	命令発行	実行中※	完了

※消去以外のアクションでは「実行中」は表示されないことがあります。

※注意	タイマーロックの履歴は残りません。
-----	-------------------

ステータスの解説

ステータス表示	命令の通知状況	クライアントの状態	命令のキャンセル操作
命令発行	命令を受信していません	何も起きていません	可
消去中※	命令を受信済み	消去実行中	不可
消去完了	命令を受信済み	消去が完了	不可
自動消去完了	命令はありません	自動消去が完了	-
キャンセル	受信していません	何も起きていません	-

※消去時間が短い場合は[消去中]ステータスが表示されないことがあります。異常ではありません。

消去命令またはリモートロック/リモートアンロックの完了時

それぞれステータスが[完了]に変わります。

コンピューター名をクリックすると[ステータスレポート]が表示され、コンピューター名、利用者名、命令の発行日時および完了日時が表示されます。

消去の場合は消去したファイル数が表示されます。

命令の実行完了時には管理者あてに[命令完了通知メール]が送信されます。

※注意	命令完了の通知を受け取るためにはコンピューターが命令実行後にネットワークに接続されている必要があります。特に消去命令では実際に消去が完了していても完了通知が管理サーバーに送られてこない場合もあります。この場合、履歴の表示は「完了」にはなりません。
※注意	消去命令を発行していないにもかかわらず消去完了通知が発行されるケースがありますが、これは自動消去が実行されたことを示します。履歴メニューには[自動消去完了]と表示されます。
※ヒント	たくさんの履歴から特定のレコードを探す場合は、検索機能を使うと便利です。検索機能は「コンピューター名」を指定する方法と、「消去年月日」を指定する方法の2通りがご利用いただけます。検索はすべて半角英数字をご利用ください。
※ヒント	不要なレコードを削除する場合は右端のチェックボックスにチェックを入れて、[削除する]ボタンを押してください。ステータスが命令発行や消去中のレコードは削除できません。
※注意	消去したファイル数はプログラムが実際に処理したデータ数を表します。消去する領域によっては見た目のファイル数だけでなく、実際には見えない付帯データを消去するため、見た目のデータ数よりも多いファイル数が表示されることがあります。

9. 位置情報取得機能

紛失したコンピューターの位置情報を地図上で確認する機能です。

動作条件

GPS 機能を搭載のコンピューター、または Windows10 および Windows8/8.1 で無線 LAN 機能を搭載するコンピューター。

位置情報を管理サーバーに通知するにはインターネットに接続する必要があります。

設定方法

設定メニューの上部にある[位置情報を利用する]にチェックを入れて[設定保存]をクリックします。

位置情報の確認方法

ホームメニューからコンピューターを選択してクリックします。詳細情報画面が開いたら下部の[位置情報を表示]ボタンをクリックします。

設定: 設定A01 ▼ [設定保存] [キャンセル]

コンピューター名: PC-006

解除パスワード: 0000

利用者: KATO

所属グループ: 営業部 ▼

備考:

電話番号:

機種品番: CF-SX3EFRTS

製造番号: 3IKSA00924

プログラムVer: Ver. 8.0.68.0

登録日時: 2015-08-13 17:40:55

2015-08-18 14:20:14 消去命令 キャンセル

アンロック

Click!

以前の画面を見る

位置情報を表示

別ウイ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 15 件の位置が表示されます。

TRUSTDELETE Biz

コンピュータ情報

コンピュータ名	製造番号	利用者
CF-SX3EFRTS	3IKSA00924	

位置情報履歴

No.	計測日時	緯度	経度	精度(m)
1	2014/12/08 16:33:20	35.686238	139.696638	61
2	2014/12/05 17:03:25	35.686240	139.696641	55
3	2014/12/05 16:46:23	35.686243	139.696639	55
4	2014/12/05 16:35:20	35.686243	139.696637	55
5	2014/12/05 16:18:18	35.686239	139.696639	55
6	2014/12/05 16:03:16	35.686242	139.696641	55
7	2014/12/05 15:48:15	35.686242	139.696642	55
8	2014/12/05 15:33:13	35.686241	139.696641	55
9	2014/12/05 15:18:11	35.686244	139.696637	55
10	2014/12/05 15:01:40	35.686244	139.696634	55
11	2014/12/05 15:00:54	35.686241	139.696635	55
12	2014/12/05 12:07:52	35.686238	139.696638	61
13	2014/12/05 12:07:37	35.686238	139.696638	61
14	2014/12/05 11:25:25	35.686242	139.696636	55
15	2014/12/05 11:16:23	35.686241	139.696638	55

コンピューターが稼働中に位置情報取得を定期的に行いますが、インターネットに接続するまでは取得した情報を管理サーバーに通知することはできません。

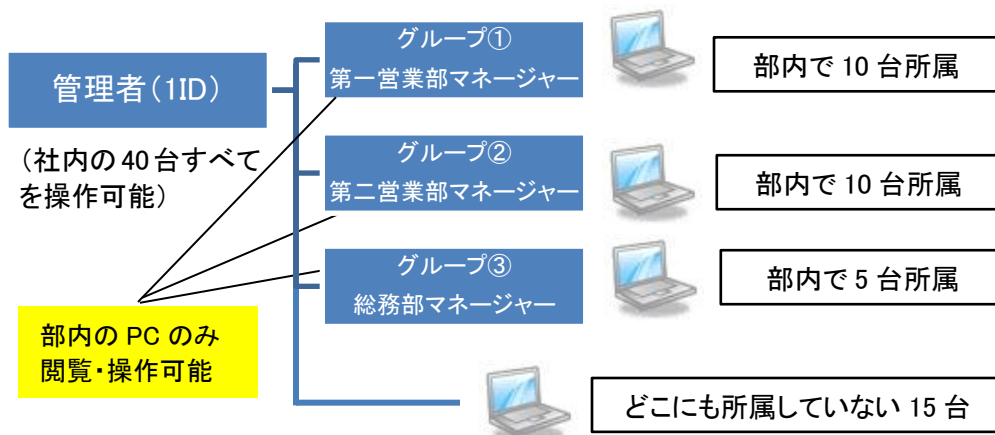
同じ緯度、経度、精度の位置情報が連続して送られてきた場合には、表示はまとめられます。

コンピューターに割り振られた IP アドレスが位置情報データベースとリンクしていない場合、実際の位置とは異なる情報が地図上に表示されることがあります。

10. グループ管理機能

グループ管理機能とは

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保護すべきデータ量や保存場所が異なります。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、各部署(グループ)の責任者による個別管理が可能です。



各グループ責任者は自分の管理下のコンピューターのみ操作することが可能

※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、本機能の設定は必要ありません。
------	--

グループ管理機能でできること

- ◆ グループを複数作成し、各コンピューターをそれぞれのグループに登録することで、企業内のコンピューターを部署単位で管理可能。
- ◆ コンピューターまたはそのユーザーの配属が変わる場合、該当するコンピューターを別のグループに配置換えすることができます。

管理者とグループ責任者の権限の違い

管理者

- ◆ 管理サーバーのすべての機能を操作できます。
- ◆ 企業内のすべてのコンピューター(グループの所属の有無に関わらず)に対して対象設定の作成・変更、消去の発行・停止、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。

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、位置情報の確認、履歴の閲覧等を実行できます。

グループ責任者アカウントの制限事項

- ◆ [設定]、[管理者]、[グループ管理]メニューは利用できません。
- ◆ 所属グループが異なるコンピュータ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の所属グループを設定または移動できません。
- ◆ 登録されているコンピュータの登録解除はできません。
- ◆ 登録されているコンピュータの詳細情報の変更はできません。

グループ管理機能を使う前の準備

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。[グループ管理]のメニューで[グループ一覧]内の[新規登録]ボタンを押し、登録画面でグループ名を登録します。

続いて[管理者一覧]内の[新規登録]ボタンを押し、登録画面でグループ責任者のログイン ID とパスワードを入力し、管理対象とするグループを選択します。[登録]ボタンを押すと作成したグループ責任者が[管理者一覧]に表示されます。管理者も同様の手順で追加することができます。

※注意

- ・グループ名は最大 25 文字まで入力できます。
- ・ログイン ID は 8～16 文字の半角英数字になります。
- ・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 1 契約当たり、50 個まで作成できます。
- ・管理者、グループ責任者は 1 契約当たり、合計で 50 個まで発行できます。
- ・グループ責任者や管理者のログイン ID、パスワード、管理対象グループを変更する際は、ログイン ID をクリックして編集画面を表示してから変更してください。
- ・ログイン中の管理者の管理対象グループは変更できません。
- ・ログイン中の管理者は削除できません。

所属グループの指定方法

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。

ホームメニューでコンピューターを選択してクリックします。詳細情報画面が表示されたら[所属グループ]のプルダウンから任意のグループ名を選択して、[設定保存]ボタンを押します。

The screenshot shows a configuration window for a computer. The '所属グループ' (Assigned Group) field is highlighted with a red box, and its dropdown menu is open, showing three options: '営業部' (Sales Dept.), '経営部' (Management Dept.), and '開発部' (Development Dept.). The '営業部' option is currently selected. Other fields include '設定' (Setting) set to '設定A01', 'コンピューター名' (Computer Name) 'PC-006', '解除パスワード' (Release Password) '0000', '利用者' (User) 'NATO', '機種品番' (Model No.) 'CF-SX3EFRTS', '製造番号' (Serial No.) '3IKSA00924', 'プログラムVer.' (Program Ver.) 'Ver. 8.0.68.0', '登録日時' (Registration Time) '2015-08-13 17:40:55', '最終履歴' (Final History) '2015-08-18 14:20:14 消去命令 キャンセル', 'ロック状態' (Lock Status) 'アンロック', and 'タイマーロック解除' (Timer Lock Release). Buttons for '設定保存' (Save Setting) and 'キャンセル' (Cancel) are visible at the top right.

以上の設定が完了したらグループ責任者に専用ログイン ID とパスワードを通知します。責任者がグループ専用ログイン ID とパスワードでログインするとグループ配下のコンピューターだけが表示され、操作可能となります。使用できるメニューや機能も制限されます。

所属部署を決定または変更するときの注意事項

- ◆ グループを変更しても対象設定（消去の対象や認証間隔など）はそのままの設定が引き継がれることとなります。部署ごとに独自の対象設定を使用している場合は、異動先の対象設定に変更することが必要です。グループ名を変更した場合は必ず対象設定を見直して正しく設定するよう注意してください。
- ◆ 消去命令を発行中のコンピューターはグループの指定や移動はできません。消去が完了してから再度設定を行ってください。
- ◆ 部署異動などでコンピューターの所属グループが変わる場合は、新しいグループの ID を上書きして設定を保存してください。
- ◆ コンピューターを所属のグループから外す場合は、グループ名を空にして[設定保存]を実行してください。グループ名を空にすると、コンピューターは再び管理者の直轄管理下に配置されます。

1 1. その他の機能

ログイン時間制限

ログイン後、操作せずに 30 分が経過すると自動でログアウトします。

コンピューター検索機能

複数台でご利用の場合、管理サーバーのコンピューター管理メニュー(トップ画面)の一覧表示で、任意のコンピューターを検索することができます。検索方法は次の 2 種類が利用できます。

- ◆ キーワード指定で検索(左):コンピューター名または利用者氏名、備考欄による検索。検索キーワードと部分一致した項目が一覧で表示されます。
- ◆ 接続日時で検索(右):一定時間サーバーと認証していないコンピューターを検索できます。画面右上の検索ウインドウにカーソルをあてるとカレンダーが表示されます。最終認証日を選択すると、その日付以降に認証していないコンピューターが一覧表示されます。
- ◆ 検索条件をクリアするにはリスト左上の「表示をリセット」ボタンをクリックしてください。

※注意	接続していないコンピューター検索に未来の日付を入力するとすべての登録情報が表示されます。入力欄には年月日を半角数字で指定してください。
※ヒント	接続していないコンピューターの検索を定期的に行うことで、サーバーへの接続頻度を把握しておくことで運用に便利です。

ソート機能

画面では登録コンピューターの表示をソート機能で並び替えることができます。並び替えの基準となる項目は[コンピューター名]、[利用者]、[ステータス]、[所属グループ]、[備考]、[最終接続日時]です。クリックを繰り返すと並びが逆転します。リスト左上の[表示をリセット]をクリックすると元の順番に戻ります。

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空きが必要な場合

登録解除の手順

画面右側のボックスにチェックを入れてから[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	登録解除ボタンをクリックする前に右端のボックスに必ずチェックを入れてください。
-----	---

登録解除のあと、空きが出たら再インストールまたは別のコンピューターを新規にインストールして登録を実行してください。インストールと登録についてはクライアントマニュアル参照してください。