

法人向けセキュリティサービス

マイセキュア ビジネス

(利用マニュアル)

第 2.4 版

2023/09/14

4. 運用中の操作	19
【1】 オンラインマニュアルについて.....	19
5. その他.....	19
【1】 管理者の追加	19
【2】 所属管理コンソールの変更方法（トライアルから継続利用のお客様）	22

はじめに（必ずお読みください）

本マニュアルは、法人向けセキュリティサービス利用規約上に規定される機密情報の一部をなすものです。本マニュアルの取り扱いにつきましては、当該規定に従い、十分ご注意ください。

■マイセキュア ビジネス ご利用の流れ

新規開設時：

①アカウントの作成（目次1（前半）参照）

「アカウント開通案内メール」に従いサービスアカウントを作成します。



②管理コンソールにログイン&初期設定(目次1（後半）参照)

「マイセキュア ビジネス」を端末へインストールする前の準備作業です。
端末を一元管理するためにグループ、セキュリティポリシーなどを設定します。



③ライセンス数の確認(目次2 参照)

「お申込内容のとおり」にライセンス数に変更されているか確認します。



④端末へのインストール(目次3 参照)

「マイセキュア ビジネス」を端末にインストールするだけで監視が始まります。
※端末によってインストール方法が多少異なります。詳しくは次頁以降をご参考ください。

ライセンス変更時：

①変更後ライセンス数の確認(目次2 参照)

お申込内容のとおり」にライセンス数に変更されているか確認します。



②端末へのインストール/アンインストール(目次3 参照)

変更ライセンス数に応じて端末へのインストール/アンインストールを行います。

運用中の操作：

①管理画面の操作(目次4 参照)

オンラインマニュアルを参考に、管理画面情報の操作を適宜実施します。

ご解約時：

①ご解約(廃止)時に特別な作業は必要ありませんが、念の為解約日前に全端末へのアンインストールの手順（目次2 参照）を実施していただくことをお勧めいたします。

1. 新規開設時の管理画面設定

【1】アカウントの作成

アカウント開通案内メール受信

①サービス開通日に合わせ送信される、「アカウント開通案内メール」の受信を確認します。

※アカウント開通案内メール（英語または日本語で受信）について

・お申込み時にご連絡いただいたメールアドレスに届いた、以下「件名／差出人」のメールです。

○件名： ウェブルート コンソールの確認 (アクションが必要)

○差出人： Webroot Console Confirmation <noreply@webrootanywhere.com>

アカウント作成ページにアクセス

②アカウント開通案内メールに記載された URL をクリックし、「アカウントの作成」ページにアクセスします。

「アカウント開通案内メール」

①件名

①差出人

②アカウント作成ページ (URL)

仮パスワード (以降の手順で使用)

The screenshot shows an email interface with the following content:

- Subject:** ウェブルート コンソールの確認 (アクションが必要)
- From:** Webroot Console Confirmation <noreply@webrootanywhere.com> (宛先: sample000@xxx.com)
- Date:** 2021/06/01
- Body:**
 - 弊社製品をご利用いただき誠にありがとうございます。
 - 登録を完了し、ウェブルート コンソールをアクティブにするには、次の確認のリンクをクリックしてください：
 - <https://my.webrootanywhere.com/regconfirm.aspx?LEX=e93d3432-d984-45af-8ab2-24b92e967adc&LXXXXXXXXXXXXXXXXX=N&AP=Y&Langs=JA>
 - 自動的に生成されたパスワードは次のとおりです： **cRYW9099dvcY99P**
 - ぜひ近日中にウェブルートをご利用ください。
 - 今後ともご愛顧のほどよろしくお願い申し上げます。
 - ウェブルート株式会社

「登録確認(アカウントの作成)」画面の項目を入力

①「登録確認(アカウントの作成)」ページに必要情報を入力し、「今すぐ登録」をクリックします。

「登録確認画面 (アカウントの作成画面)」

・パスワードは9文字以上、最低でもアルファベット6文字と数字3文字を含む必要があります。
・また、特殊文字(<>を除く)も使用できます。

・6文字以上の覚えやすい言葉や数字を入力ください。
(ログイン時毎回このコードのうち2文字の入力を求められます。)

※②のパスワード、④の個人用セキュリティは以降のログイン時に必ず必要となります。

※⑥のセキュリティの質問の回答は、パスワード紛失時に必要となります。

・入力完了後、「今すぐ登録」をクリックすると登録完了画面が表示されます。

「登録完了 画面」

以上で、アカウント作成は完了です。

引き続き管理コンソールへログインするため、「ログイン」をクリックします。

【2】管理コンソールへのログイン

端末へ「マイセキュア ビジネス」をインストールする前に、管理コンソールへログインし、セキュリティポリシーの指定など初期設定を行います。

- ① 「ログインする」画面に必要な情報を入力し、「ログインする」をクリックします。

「管理コンソール ログイン画面（ログインする画面）」

・操作前にログインする画面であることを確認する



The screenshot shows the Webroot login page. At the top, there is a 'ログインする' (Login) button and an 'アカウントを作成する' (Create account) button. Below these are input fields for '電子メールアドレス/電話番号' (Email/Phone number) and 'パスワード' (Password). The 'ログインする' button is highlighted with a red dashed box. At the bottom, there is a language selection dropdown menu currently set to '日本語' (Japanese), also highlighted with a red dashed box. Annotations with blue callout boxes provide instructions: 'アカウント作成時に決めたパスワードを入力' (Enter the password you decided when creating the account) points to the password field; '英語表記の場合は、こちらから日本語に変更ください。' (If in English characters, please change to Japanese from here) points to the language dropdown; and '上記①、②をすべて入力したあと、「ログインする」をクリック' (After entering all the above ① and ②, click 'Login') points to the login button.

・アカウント作成時に決めたパスワードを入力

・英語表記の場合は、こちらから日本語に変更ください。

- ② 「コンソールに進む」をクリックします。(ご利用環境により表示されない場合があります)

「管理コンソール ログイン画面」



The screenshot shows the Webroot console page. At the top, there is a 'サインイン済み' (Signed in) status. Below this is a green icon with a white 'W' and a 'コンソールに進む' (Go to console) button, which is highlighted with a red dashed box. At the bottom, there is a language selection dropdown menu currently set to '日本語' (Japanese).

③セキュリティコードの確認を求められるので、入力後ログインします。

「管理コンソール ログイン画面」

・アカウント作成時に決めた
セキュリティコードを入力

④ 2段階認証の設定に関する画面が表示されます。

必要により「2FAを設定する」をクリックして、2段階認証の設定を行ってください。
(以降の2段階認証の設定手順は後述<参考>を参照ください)

※2段階認証の利用には、スマートフォンまたはタブレットが必要となります。また、ご用意頂いた端末に認証用アプリのインストールも必要となりますので、事前に端末のご準備及び認証用アプリのインストール可否の確認を、お願いします。

⑤本手順では、「今はスキップする」をクリックして先へ進みます。

「2段階認証の設定画面」

⑥管理コンソールのホーム画面が表示されます。

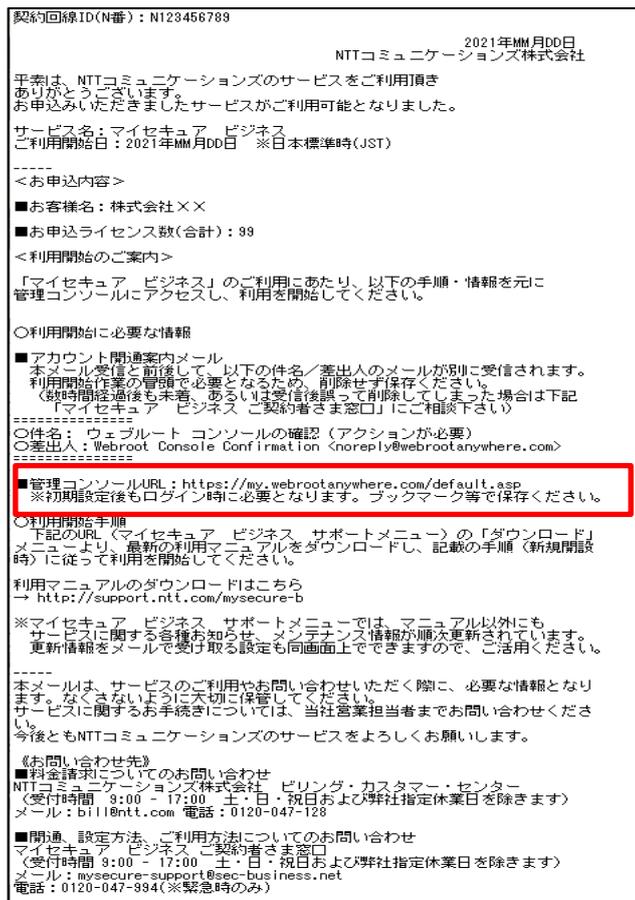
「管理コンソール ホーム画面」



以上で管理コンソールへのログインは完了です。

※以降の運用で管理コンソールへログインする場合は、管理コンソール URL(アカウント開通案内メールと同時に送付される「サービス提供開始のお知らせ」メールに記載されています)へアクセスし、本手順「管理コンソールへのログイン」に沿ってログインください。

「サービス提供開始のお知らせ」



引き続き、セキュリティポリシーなど必要な初期設定を行います。

<参考> 2段階認証の設定手順

2段階認証を設定する場合、「2FA を設定する」クリック後の手順は以下の通りです。

- ①ステップ1：デバイスの紛失、盗難時対策として追加で2つの質問に答え「続ける」をクリックします。

「2段階認証 設定画面（ステップ1）」

・操作を中断する場合は、必ず「キャンセル」ボタンから中断する。

画面の案内に従い、認証アプリをインストールします。

※本画面表示後、手続きを途中で中止する場合は、必ず左下の「キャンセル」ボタンを押して中止ください。

(ウィンドウ右上の「×」ボタンで閉じると、管理画面に再ログインできなくなる場合があります)

- ②ステップ2：推奨された認証用アプリのうち1つをダウンロードおよび設定をします。
- ③ステップ3：設定した認証用アプリから表示されたQRコードをスキャンし、管理コンソールを認証用アプリに登録します。

「2段階認証 設定画面（ステップ2、3、4）」

・操作を中断する場合は、必ず「キャンセル」ボタンから中断する。

- ④ステップ4：登録後、認証用アプリに表示された認証コードを入力し「認証コードを確認する」をクリックします。
- ⑤認証コード入力後【認証が成功しました】と表示されたら「設定を完了する」をクリックします

「2段階認証 設定画面（ステップ2、3、4）」



- ⑥「コンソールに進む」をクリックし、ホーム画面に戻ります。

「2段階認証 設定完了画面」



以上で2段階認証の設定は完了です。

[3] 新しいポリシーの作成

本マニュアルではデフォルトのポリシーを一部変更し、新しいポリシーを作成します。
※デフォルトのポリシーをそのままご利用する場合は本作業は省略し次のステップにお進みください。

①管理コンソールのホーム画面で「エンドポイントプロテクション」をクリックします。

「管理コンソール ホーム画面」



②管理コンソールの「ポリシー」をクリックします。

「管理コンソール ダッシュボード画面」



③「推奨デフォルト設定（:）」を選択し、「コピー」をクリックします。

「管理コンソール 管理（ポリシー）画面」



- ④「コピーするポリシー」という画面が表示されるので、「名前」と「説明」(どちらも入力必須)を入力後、変更したいポリシーを変更してください。
 ※入力後「保存」をクリックすると、ポリシーが作成されます(「戻る」から一覧に戻ります。)

「コピーするポリシー 画面」

WEBROOT | Management Console CE 22.2

コピーするポリシー: 推奨デフォルト設定

* 必須フィールドです

名前 *

①ポリシー名を入力(必須)

説明 *

②ポリシーの説明を入力(必須)

ポリシー設定 ③必要なポリシーを変更

セクション
> 基本設定
> スキャンのスケジュール
> スキャン設定
> 自己保護
> ローカル ヒューリスティック
> インターネット ヒューリスティック
> ネットワーク ヒューリスティック
> CD/DVD ヒューリスティック
> オフライン ヒューリスティック
▼ リアルタイムシールド
リアルタイム シールド有効 <input type="radio"/> オフ <input checked="" type="radio"/> オン
セキュアエニウェアの中央データベースに基づくオフライン保護を有効にする <input type="radio"/> オフ <input checked="" type="radio"/> オン
ブロックされたファイルに対するアクションを記憶する <input type="radio"/> オフ <input checked="" type="radio"/> オン
ブロックされたファイルを自動的に隔離する <input type="radio"/> オフ <input checked="" type="radio"/> オン
実行時に検出された場合ファイルを自動的にブロックする <input type="radio"/> オフ <input checked="" type="radio"/> オン
書き込みまたは変更時にファイルをスキャンする <input type="radio"/> オフ <input checked="" type="radio"/> オン

戻る ⑤「戻る」をクリック ④上記①~③の入力が完了したら「保存」をクリック 保存

<注意> ポリシーについて

- ・ポリシーを適用するにあたり、PC には「推奨デフォルト設定」、サーバーには「推奨サーバーデフォルト設定」のポリシーを利用ください。
 - ・2023 年 2 月 7 日以降「推奨デフォルト設定」内の回避シールドポリシーが、デフォルトでオン(検出と修復)設定となりました。本設定に伴い、貴社独自で作成されたプログラムなどを過検知するなど意図しない検知が増えた場合は、機能をオフにするなどお試しください。(回避シールドをオフにしても脅威検知レベルは変わりません)
- ※回避シールド：スクリプト系などのファイルに潜む脅威を早期発見するポリシーです。

以上で、新しいポリシーの作成は完了です。

【4】ポリシーの適用

新しく作成したポリシーをデフォルトのポリシーとして登録し、今後インストールされる端末全てに適用します。

- ①管理コンソールの「設定」>「エンドポイント」を開き、「デフォルトのエンドポイント ポリシー」をクリックした際に表示されるポリシーの一覧から、対象ポリシーを選択し「変更を保存」をクリックします。

「管理コンソール 設定（エンドポイント）画面」

WEBROOT Management Console CE 22.2

設定 (エンドポイント) 画面

①「設定」を選択

②「エンドポイント」をクリック

③対象ポリシーを選択(作成したポリシー)

④「変更を保存」をクリック

以上、ポリシーの適用は完了です。

2. ライセンス数の確認

ご契約後、または変更申込によりライセンス数を変更された場合、管理コンソールでライセンス数の確認を実施ください。

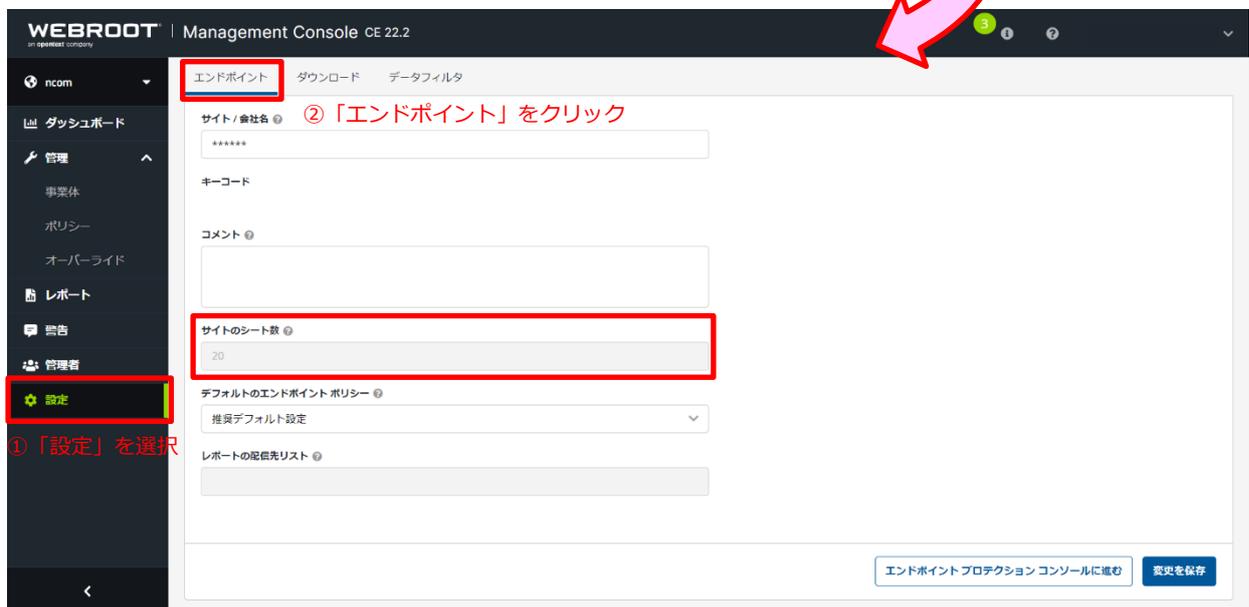
【1】ライセンス数の確認

①ホーム画面から「エンドポイント プロテクション」を選択し、さらに「設定」メニューを選択します。

「管理コンソール ホーム画面」



「管理コンソール 設定（エンドポイント）画面」



※画面上に表示されている「サイトのシート数」の値が現在の購入済みライセンス数です。
変更した際は変更後のライセンス数を一致することを確認して下さい。

以上、ライセンス数の確認は完了です。

3. 端末へのインストール／アンインストール

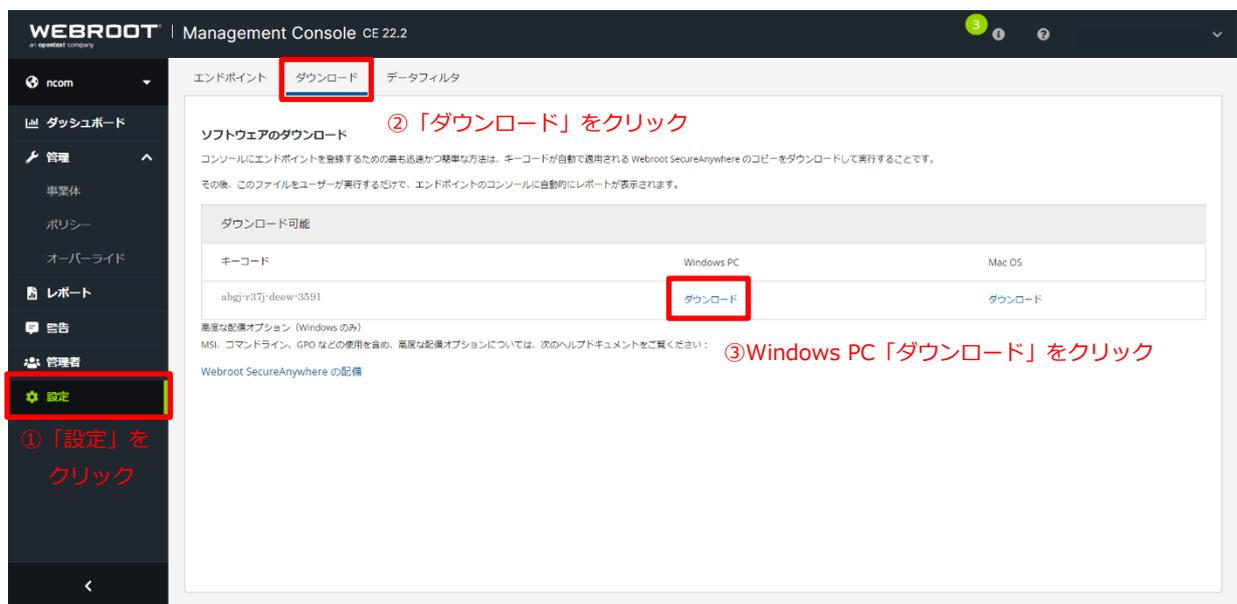
初期設定を完了し、対象端末へ「マイセキュア ビジネス」のインストールを実施します。
インストールするだけで、端末の保護は開始されます。

【1】 端末へのインストール

Windows 版

管理コンソール「設定」の「ダウンロード」をクリックすると、インストールソフトのダウンロードページが表示されます。インストール用のリソースは Windows と Mac で異なりますので任意で、お選びください。

「管理コンソール 設定（ダウンロード）画面」



- ③の Windows PC 用ダウンロード：クリックすると exe ファイルがダウンロードされます。ダウンロードしたファイルを対象の Windows 端末で実行させるとインストールが開始します。
※exe ファイルはメール添付が不可能であるため、Push ツールで一斉配信、または共有フォルダに置いて配布することを推奨します。
※「Windows 用ダウンロード」を利用する場合、インストール時のキーコード入力が不要となります。また exe ファイルを複数ダウンロードするとファイル名末尾に(1),(2)が付与されますがファイル名が変わるとキーコードが認識されなくなりますのでご注意ください。

高度な配布オプション：インストーラーを利用した配布方法です。詳細は管理コンソールからリンクされるヘルプをご参照ください。

Mac 版

同様、管理コンソールの「ダウンロード」をクリックします。

「管理コンソール 設定 (ダウンロード) 画面」



①「設定」をクリック

- ③の Mac 用ダウンロード：クリックすると dmg ファイルがダウンロードされます。ダウンロードしたファイルを対象の Mac 端末で実行させるとインストールが開始します。
※macOS バージョンに応じてダウンロードボタンを選択ください。
※dmg ファイルはメールへの添付、Push ツールでの配信、共有フォルダからの配布が可能です。

【2】インストール済み状態の確認 (端末)

インストールが完了すると、こちらのアイコン  が端末上に表示されます。

「デスクトップ画面 タスクバー」



【3】インストール済み状態の確認 (管理コンソール)

インストール完了後、「事業体」メニューの「すべての事業体」画面で、インストールした端末が表示されていればインストール完了 (管理対象) です。

「管理コンソール 管理 (事業体) 画面」



※この画面でグループの作成や、適用ポリシーの変更なども可能です。
詳しくはオンラインマニュアル「事業体」を参照ください。

【4】 アンインストール

端末からエージェントのアンインストールを行う場合は、管理コンソールから「デバイスを非アクティブ化」を行います。（管理コンソールで操作した後、「デバイスを非アクティブ化」指示を端末側で受信するのに、若干のタイムラグが発生します）

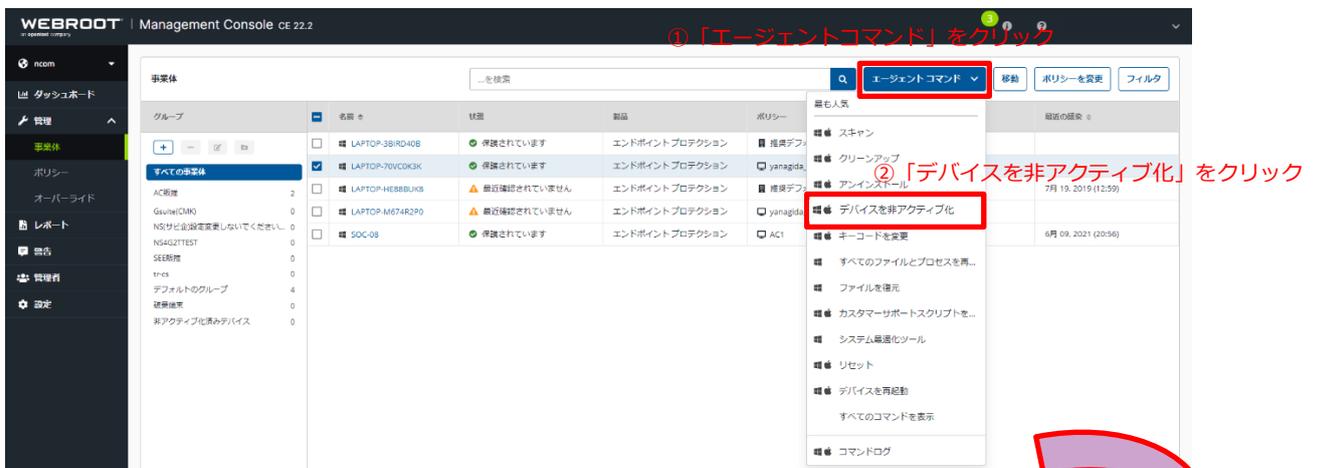
- ①管理コンソールにログインし「事業体」「すべての事業体」を開きアンインストールしたい端末をクリック（レ チェック）します。

「管理コンソール 事業体（すべての事業体）画面」



- ②「エージェントコマンド」から「デバイスを非アクティブ化」をクリックします。

「管理コンソール 事業体（すべての事業体）画面」



- ③「デバイスを非アクティブ化」の確認が表示されたら「コマンドの送信」をクリックします。

「エージェントコマンド：デバイスを非アクティブ化 ポップアップ画面」



このコマンドを送信すると、選択したデバイスから Webroot ソフトウェアを削除しようとしています。請求が正確に行われるように、コマンドが送信された後、選択した各デバイスからウェブルートソフトウェアが完全に削除されていることを確認してください。

キャンセル

①「コマンドの送信」をクリック

コマンドの送信

④ 「すべてのエンドポイント」画面上から対象端末の表示が消えたことを確認します。

「管理コンソール 事業体（すべての事業体）画面」



グループ	名前	状態	製品	ポリシー	最終検出日時	最近の感染
すべての事業体	LAPTOP-3B8RD40B	保護されています	エンドポイントプロテクション	推奨デフォルト設定	4月 22, 2022 (12:57)	
テストグループ	LAPTOP-HE888UKS	最近確認されていません	エンドポイントプロテクション	推奨デフォルト設定	2月 22, 2022 (17:31)	7月 19, 2019 (12:59)
非アクティブ化済みデバイス	LAPTOP-M674R2P0	最近確認されていません	エンドポイントプロテクション	yanagida_demo	4月 14, 2022 (23:58)	
	SOC-08	保護されています	エンドポイントプロテクション	AC1	本日 (09:49)	6月 09, 2021 (20:58)

以上でアンインストールの作業は終了です。

※上記の手順実施後、端末側で実際にアンインストールされるまでには一定のタイムラグ（最大1日程度）があります。一定期間お待ちいただき、それでも端末側でアンインストールが実施されない場合は、マイセキュアビジネスご契約者さま窓口（「サービス提供開始のお知らせ」メールに記載されています）にご相談下さい。

4. 運用中の操作

運用中の各種操作方法については、オンラインマニュアルに詳細が記載されています。
必要に応じ適宜ご参照ください。

【1】オンラインマニュアルについて

管理コンソールの詳細な操作方法については、以下のオンラインマニュアルをご参考ください。

<https://docs.webroot.com/jp/ja/business/administratorguide/administratorguide.htm#GetStarted.htm>

※管理コンソールからもアクセス可能です。

管理コンソール画面、右上にある  > をクリックください。

5. その他

【1】管理者の追加

ご利用開始時、管理コンソールを操作する管理者として、以下の管理者アカウントが設定されてます。

- ・ 開通案内を送付したメールアドレス
- ・ サービス管理用のメールアドレス

※弊社サポート用に数名程度メールアドレスが追加されております。(@ml.ntt.com のアドレスとなります)

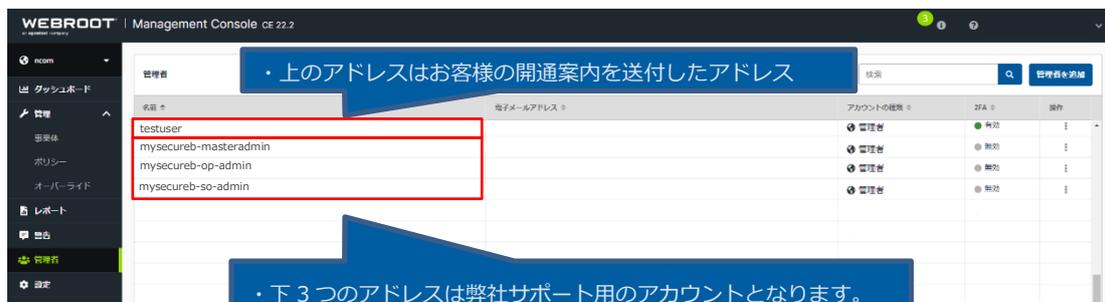
▼マイセキュア ビジネス（単体）で、ご利用の場合

用途（例）
マイセキュア ビジネス 管理
マイセキュア ビジネス サポート管理
マイセキュア ビジネス サービス管理

▼マイセキュア ビジネス（Google Workspace オプション）で、ご利用の場合

用途（例）
マイセキュア ビジネス(G Option) 管理
マイセキュア ビジネス(G Option) サポート管理
マイセキュア ビジネス(G Option) サービス管理

「管理コンソール 管理者画面」



• 上のアドレスはお客様の開通案内を送付したアドレス

名前	電子メールアドレス	アカウントの種類	2FA	操作
testuser		管理者	有効	⋮
mysecureb-masteradmin		管理者	無効	⋮
mysecureb-op-admin		管理者	無効	⋮
mysecureb-so-admin		管理者	無効	⋮

• 下3つのアドレスは弊社サポート用のアカウントとなります。

管理者のアカウントは、以下の手順によって追加することができます。

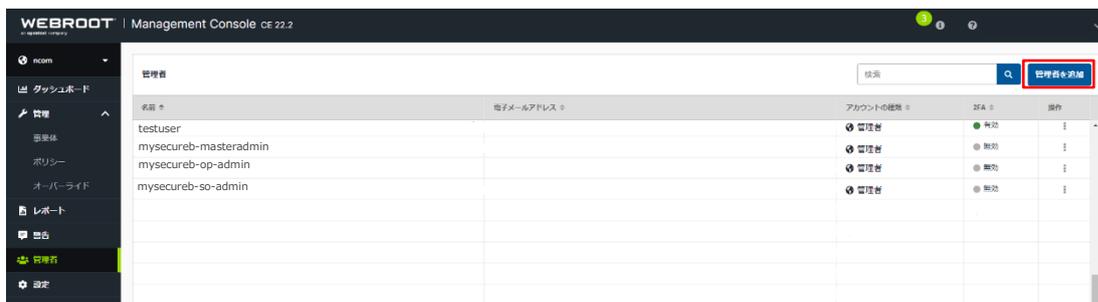
- ①管理コンソールにログインします。
- ②メニュータブの、「管理者」をクリックし、管理者画面を開きます。

「管理コンソール 管理者画面」



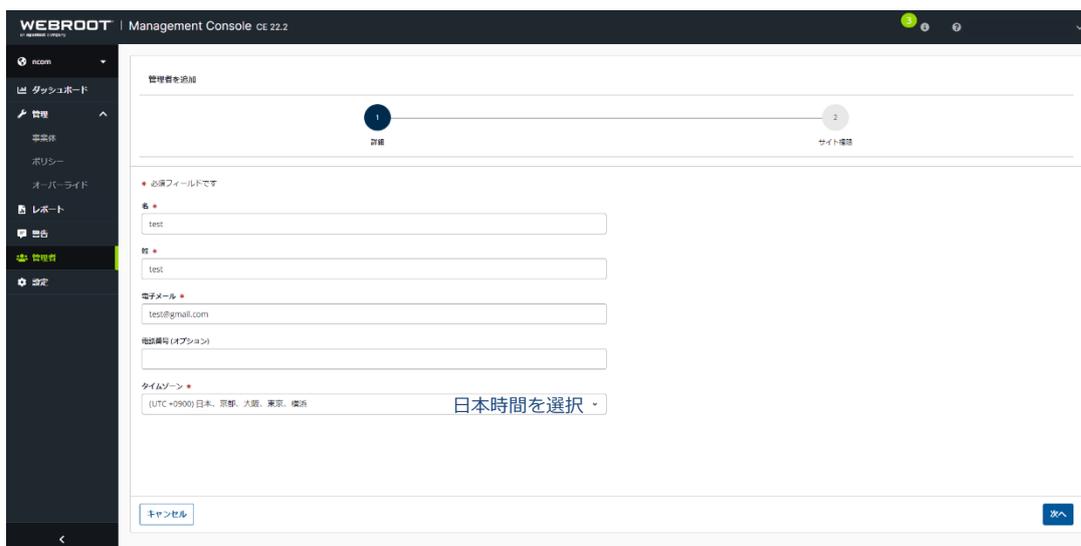
- ③「管理者を追加」ボタンをクリックし、「管理者を追加」画面を表示します。

「管理コンソール 管理者画面」



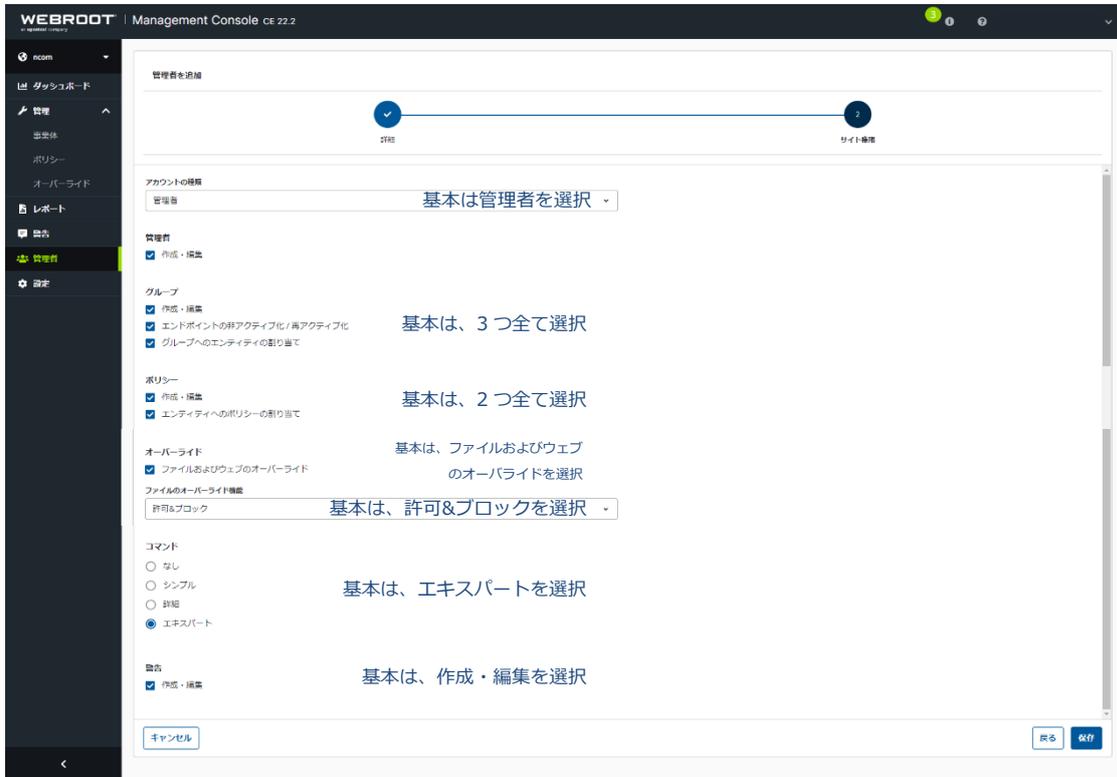
- ④詳細の必須項目を記入し、「次へ」ボタンをクリックします。

「管理コンソール 管理者（管理者を追加）画面」



④ サイト権限の必須項目を記入し、「保存」ボタンをクリックします。

「管理コンソール 管理者を追加（サイト権限）画面」



⑤ 追加後、管理者メニューが表示されるので、追加を確認します。

「管理コンソール 管理者画面」



⚠ 本人のアカウント開設が完了するまで表示されます。
※ ⚠ にカーソルを合わせると「確認の電子メールを再送信」という名称のリンクが表示され再送することが可能です。

以上で管理者の追加作業は終了です。

【2】所属管理コンソールの変更方法（トライアルから継続利用のお客様）

ある管理コンソールでインストールした端末をアンインストールせず、そのまま別の管理コンソールへ所属変更させることができます。この手順によりトライアル用でインストール済みの端末をアンインストールせず、そのまま本契約用の管理コンソールへ所属させることも可能ですのでご活用下さい。

- ①所属替えする場合は、各管理コンソールに付与されたキーコードを使用します。
新しく所属する管理コンソールの「設定」メニューに表示されているキーコードを確認・記録してください。

「管理コンソール エンドプロテクション（設定）画面」

WEBROOT | Management Console CE 22.2

エンドポイント ダウンロード データフィルタ

サイト/会社名

キーコード
0000-XXXX-1111-YYYY-22ZZ ②キーコードの記録（メモ） キーコード(20桁の英数字(‘-’つなぎ))

コメント

サイトのシート数
20

デフォルトのエンドポイントポリシー
推奨デフォルト設定

レポートの配信先リスト

①設定メニューを選択

エンドポイントプロテクションコンソールに進む 変更を保存

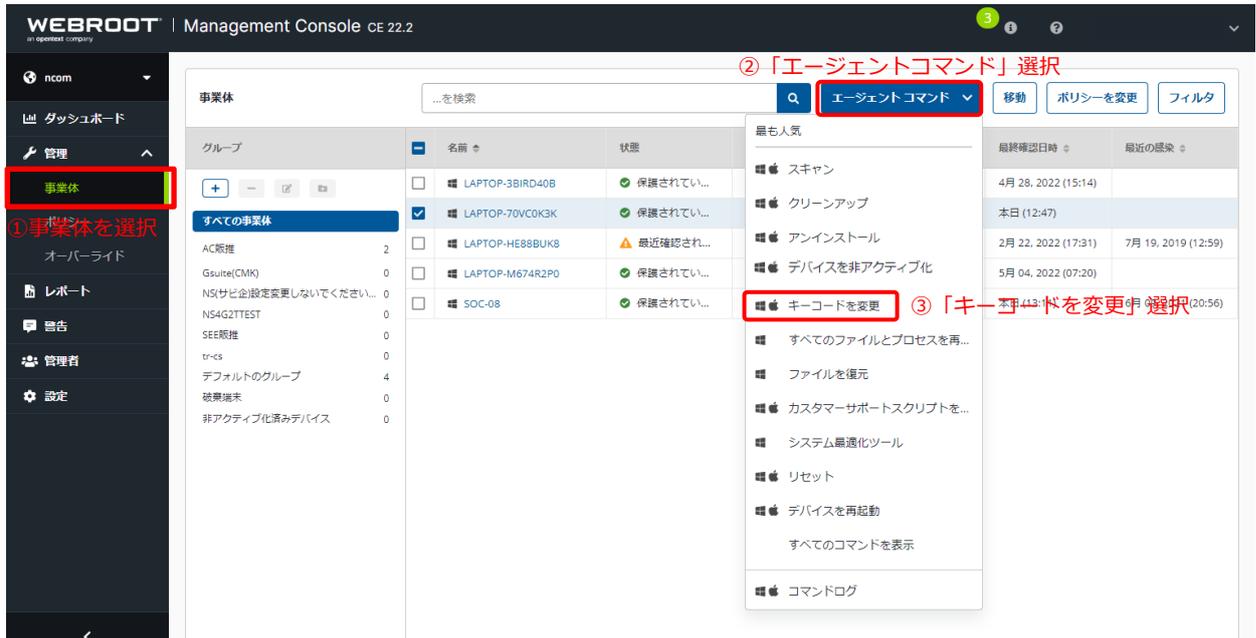
- ②現在端末が所属している（変更前の）管理コンソールにログインします。
※トライアルから変更の場合、トライアルで使用していた管理コンソールになります。

クライアント端末側のキーコード切り替え(PC 端末)します。
最初に確認・記録したキーコードを使用し、管理コンソールより遠隔コマンドで所属先を切り替えます。

- ③管理コンソールの「事業体」より、切り替えたい端末を選択します。

④「エージェントコマンド」⇒「キーコードを変更」をクリックしてください。

「管理コンソール 管理（事業体）画面」



⑤新しい所属先のキーコードを入力します。

「キーコードを変更 ポップアップ画面」

エージェントコマンド: キーコードを変更

① コマンドはデバイスに対してのみ実行できます。

選択したデバイスに別のキーコードを指定します。

* 必須フィールドです

キーコード *

0000-XXXX-1111-YYYY-22ZZ ①キーコードを入力

②「コマンドの送信」をクリック

キャンセル **コマンドの送信**

「コマンドの送信」をクリックすると、選択した端末にコマンドが送信され、端末がコマンドを受信したタイミングでキーコードの切り替えが完了します。

※キーコードの切り替えがなかなか完了しない場合、端末側でコマンドの受領が未完の場合があるため、コマンドを送信した端末画面の上のアイコンを右クリックし、「設定のリフレッシュ」を選択/実施ください。（それでも完了しない場合、サポートにお問合せ下さい）