#### 目次



<u>デバイス ID 証明書をインストール</u> … P2 ~ P8

デバイス ID ルート認証局の信頼設定 ... P9 ~ P13

「Cybertrust DeviceiD Importer」の起動について … P14

最後に ··· P15

※本手順の操作には macOS の管理者権限が必要です。

※OS のバージョンにより、表示される画面が本手順と異なる場合がありますが、その場合は読替えて手順を進めてください。



- 1. 「アプリケーション」内の 「Cybertrust DeviceiD」をダブルクリックして、 「Cybertrust DeviceiD Importer」を起動します。
  - ※システム環境のアプリケーション実行許可に関する設定によっては、起動時に確認ダイアログが表示されたり、アプリケーションが起動できない場合があります。その場合は、こちらの手順を行ってから次の手順を進めてください。

• • •	く > アプリケーション	
よく使う項目	名前	
AirDrop	Android Studio	
② 最近の項目	🔥 App Store	
♣ アプリケーション	Apple Configurator 2	
	Automator	
□ デスクトップ	DeviceiD Importer	
<b>書</b> 類	F5Access	
	FaceTime	
	Font Book	
iCloud	Google Chrome	
	Launchpad	
iCloud Drive	Mission Control	
亡 共有	Photo Booth	



 「お知らせメール」に記載されている 「証明書識別子」をコピーし、 「Cybertrust DeviceiD Importer」の 「証明書識別子」欄に貼り付け、[証明書登録] を クリックします。

※デバイス ID 証明書の取得には、数秒から数十秒かかります。 しばらくお待ちください。

■ 「お知らせメール」の例

•

■■ ステップ2 ■■

「Cybertrust DeviceiD Importer」を起動し、表示された画面の内容にしたがって、 デバイスIDをインストールしてください。

なお、アプリの画面に表示された「証明書識別子」欄には、以下の文字列をコピーして貼り付けてください。

証明書識別子: DiD|G4/DeviceiD\_OSX|123456789012345

● ● Cybertrust DeviceiD Importer

「デバイスID発行のお知らせ」メールに記載されている
「証明書識別子」をコピー&ペースト、または入力し、
「証明書登録」ボタンをクリックしてください。
端末を確認した後、デバイス証明書を自動で登録します。
証明書識別子

DiD|G4/DeviceiD\_OSX|

<u>証明書登録</u>



- 「認証コード」の入力画面が表示された場合は、 「お知らせメール」の「認証コード」をコピーし、 「認証コード」欄に貼り付けて[送信] をクリック します。
  - ※「認証コード」がメールに記載されていない場合や入力画面が表示されない場合は、次の手順に進んでください。
  - 「お知らせメール」の例

-----

#### ■■ ステップ2 ■■

「Cybertrust DeviceiD Importer」を起動し、表示された画面の内容にしたがって、 デバイスIDをインストールしてください。

 $\sim\sim\sim\sim$ 

なお、アプリの画面に表示された「証明書識別子」欄および「認証コード」欄には、 以下の文字列をコピーして貼り付けてください。

証明書識別子: DiD|G4/DeviceiD\_OSX|123456789012345

認証コード: XXXXXXXX

-----





4. macOS の管理者パスワードを入力して [OK] を クリックします。





デバイス ID 証明書が自動でインストールされます。
 インストール完了後、以下のウィンドウが表示されますので、[OK] をクリックします。





6. ウィンドウ左上の赤い閉じるボタン⊗をクリックして、「Cybertrust DeviceiD Importer」を終了します。





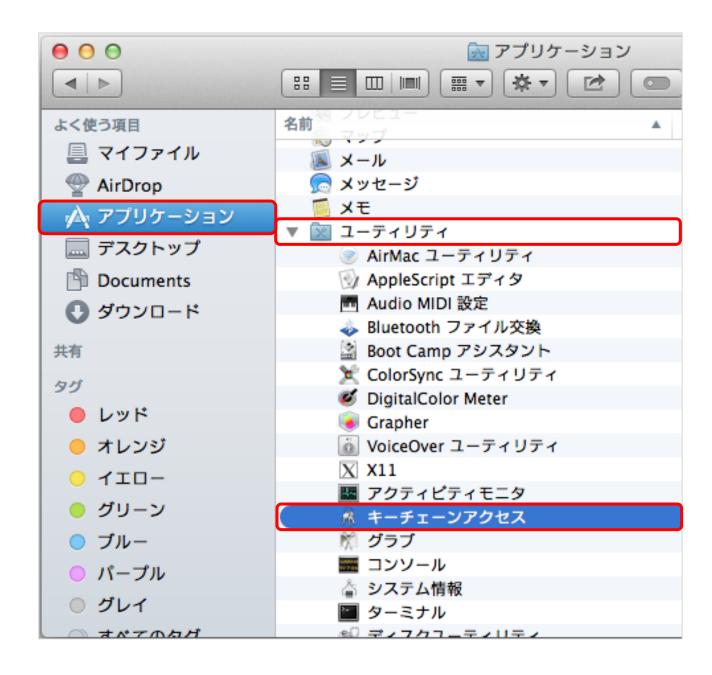
7. [はい] をクリックして、「Cybertrust DeviceiD Importer」を終了します。



デバイス ID 証明書のインストールは以上で完了です。 続いて、デバイス ID ルート認証局の信頼設定を行い ます。

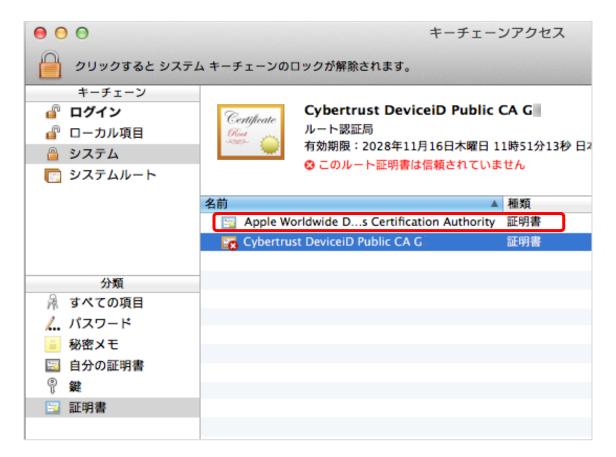


1. 「アプリケーション」、「ユーティリティ」、 「キーチェーンアクセス」の順にクリックします。





2. 「システム」を選択し、認証局証明書の一覧を表示し、認証局証明書の一覧からデバイス ID のルート認証局証明書をダブルクリックします。



※複数のデバイス ID ルート認証局証明書が表示された場合は、 それぞれのルート認証局証明書に対して、次ページ以降の手順 「デバイス ID ルート認証局の信頼設定」の 3 ~ 5 を実行し てください。

デバイス ID のルート認証局証明書は以下です。

• 第四世代認証局: Cybertrust DeviceiD Public CA G4

• 第三世代認証局: Cybertrust DeviceiD Public CA G3

• 第二世代認証局: Cybertrust DeviceiD Public CA G2



 「この証明書を使用するとき」を「常に信頼」に 変更して、ウィンドウ左上の赤い閉じるボタン ▼ でウィンドウを閉じます。

⊖ ( ) Cybertrus	t DeviceiD Public CA G	
Cybertrust DeviceiD Public CA G ルート認証局 有効期限: 2028年11月16日木曜日 11時51分13秒 日本標準時 ・ このルート証明書は信頼されていません ▼ 信頼		
この証明書を使用するとき:	常に信頼	• ?
SSL (Secure Sockets Layer)	常に信頼	<b>‡</b>
安全なメール(S/MIME)	常に信頼	<b>‡</b>
拡張認証 (EAP)	常に信頼	<b>‡</b>
IP Security (IPsec)	常に信頼	<b>‡</b>
iChat セキュリティ	常に信頼	<b>‡</b>
Kerberos クライアント	常に信頼	<b>‡</b>
Kerberos サーバ	常に信頼	<b>‡</b>
コード署名	常に信頼	<b>‡</b>
タイムスタンプ	常に信頼	<b>‡</b>
	AL :- I - AT	



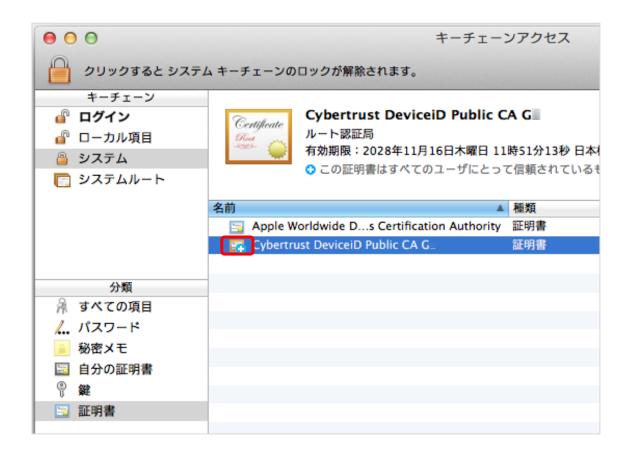
4. macOS の管理者パスワードの入力画面が表示されますので、パスワードを入力して [設定をアップデート] をクリックします。

証明書信頼設定に変更を加えようとしています。 これを許可するには、パスワードを入力してください。
名前: パスワード: ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
キャンセル 設定をアップデート



 名前の左にあるアイコンが □ の証明書は、その 証明書が信頼されていることを表します。

デバイスID のルート認証局証明書がすべて信頼されていることを確認してください。



## 以上ですべての手順は完了です。

#### 「Cybertrust DeviceiD Importer」の起動について



#### ■ 確認のダイアログが表示された場合

1. [開く] をクリックします。



#### **■ 「開けません」と表示された場合**

1. [OK] をクリックして、ダイアログを閉じます。



- 2. <u>手順1の「アプリケーション」</u>の画面で、「Cybertrust DeviceiD」をControl キーを押しながらクリックします。
- 表示されるメニューから「開く」を選択すると、以下の確認ダイアログが表示されますので、「開く」をクリックします。



#### 最後に



このドキュメントに関する著作権は、サイバートラスト株式会社に 独占的に帰属します。

このドキュメントに記載されている内容は、予告なしに変更される 場合があります。

サイバートラスト株式会社は、このドキュメントに誤りが無いことの保証は致し兼ねます。

このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。

ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。