

クレジットカード本人認証サービス(3Dセキュア2.0)



「3Dセキュア2.0」とは？

インターネット上でのクレジットカード決済時に、カード情報(カード番号/有効期限)に加えてワンタイムパスワードなどを用いた本人認証を行うことで、不正利用を防止するサービスです。

※認証方法はカード発行会社によって異なる場合があります。

(※認証方法：パスワード入力・生体認証など)

3Dセキュア2.0の利用方法

1.カード発行会社で
事前登録を行う



2.決済ページでカード
情報を入力する



3.カード会社が発行する
ワンタイムパスワードを受取る

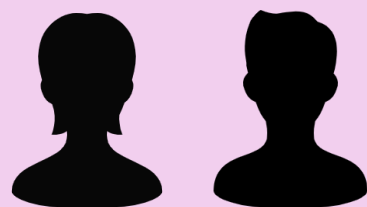


4.認証画面でワン
タイムパスワード
を入力する



※事前登録・登録方法は、各カード発行会社へお問い合わせください

会員様(購入者)



3Dセキュア対応
クレジットカードを利用

あすなろ投資顧問(加盟店)



①弊社サイトにおいて
有料商品の購入時に
クレジットカード決済を
選択

②決済ページにて
クレジットカード情報入力



クレジットカード
ブランド

⑥パスワード入力
【認証完了】



⑤パスワードなどの
追加認証要求画面



クレジットカード発行会社

④リスクレベルを判定

高リスク→追加認証（ワンタイムパスワード等）→⑤へ
低リスク→パスワード入力不要→【認証完了】→⑦へ

③本人認証要求

⑦認証結果【決済完了】



3Dセキュア2.0の名称は各ブランドによって異なります

- Mastercard** : 「Mastercard SecureCode」
Visa : 「Visa Secure / 旧：VISA認証サービス」
JCBカード : 「J/Secure™」
American Express : 「SafeKey（アメリカン・エクスプレス・セーフキー）」
Diners Club : 「ProtectBuy（プロテクト・バイ）」

The image displays three separate authentication screens for different credit card brands, all requiring a password or code for verification.

- Visa Screen:** Titled "Verified by VISA". It asks the user to enter a password. The screen shows transaction details: 加盟店: MusicWorld, ご利用金額: \$23.14, ご利用日: 6/11/2001, カード番号: **** * 9010. There is a red box around the password input field.
- Mastercard Screen:** Titled "MasterCard SecureCode". It asks the user to enter their SecureCode. The screen shows transaction details: 加盟店名: Golf Shop, 利用金額: \$250.00, 利用日: 07-20-2002, カード番号: XXXXX XXXXX XXXXX 0011, 専用グリーティング: こんにちは！花子さん. There is a red box around the SecureCode input field.
- JCB Screen:** Titled "JCB J/Secure GlobalCard". It asks the user to enter their J/Secure™ (パスワード) code. The screen shows transaction details: 加盟店名: ABCフラワーショップ, ご利用金額: JPY 10,000, ご利用日: 2003/9/26, カード番号: XXXX XXXX XXXX 9912, パーソナルメッセージ: ハワイズ好き. There is a red box around the password input field.

※3Dセキュア2.0に関する注意事項※

3Dセキュア2.0の登録は、カード発行会社の会員サイトやアプリで行うものです。
登録には、IDやパスワードのほか、ワンタイムパスワードの発行に必要な携帯電話番号やメールアドレスの登録が必要な場合があります。

3Dセキュア2.0の認証方法は、カード発行会社によって異なります。
また、本人確認が不要と判断された場合はパスワードの入力画面が表示されない場合があります。

3Dセキュア2.0は、第三者による「なりすまし」などの不正利用を防ぐためのサービスです。
フィッシング詐欺が発生しているため、メールやSMSからのお手続きでクレジットカード情報等の入力を求められる場合はご注意ください。