多要素認証
サプライヤー向けガイド

Coupa Software, Inc.

本文書の変更点

更新日時	更新種別	更新概要	詳細
2024 年 4 月 17 日	新規	新規作成	本マニュアルを新規作成
2024 年 6 月 19 日	更新・追加	・名称の変更統一 ・補足説明を追記	・「二要素認証」を「多要素認証」に変更統一 ・COUPA における多要素認証に「ユーザーの追加」を追記

目次

本書の目的および留意事項

- お取引先バイヤー企業とのお取引において Coupa Supplier Portal（CSP）をお使いのサプライヤーを対象とした資料となります。
- 多要素認証の設定方法やポータルへの再アクセスが必要な時の手順およびコンタクト先の情報についてご説明いたします。
- お取引内容や運用に関するお問い合わせにつきましては、お取引先バイヤー企業に直接ご連絡ください。

<u>免責事項</u>

- 本資料の内容は、事前に予告することなく、変更、修正し、また削除することがあります。弊社はこれらについて、何ら責任を負うものではありません。
- 本資料に掲載されている情報の正確性には万全を期しておりますが、技術上または法令解釈上など不正確な記載や誤植を含む場合があります。情報が不正確であったこと、あるいは誤植があったことなどにより生じたいかなる損害に関しても責任を負いません。

多要素認証の概要

多要素認証とは

ログインを許可する処理にあたる認証において、認証の三要素（知識、所有、生体）のうち、異なる複数の要素を組み合わせて本人確認を行う認証方法を指します。
認証の要素を増やすことでログイン時の本人確認の精度と安全性を高める方式です。

Coupa における多要素認証

COUPA における多要素認証は、法人、支払先の設定およびユーザーの追加を行う際に必須です。
ログイン時の多要素認証は任意となりますが、セキュリティを強化するという観点から設定が推奨されます。
また特定の顧客では、多要素認証を顧客情報のアクセス時に必須としている場合もあります。
認証の三要素のうち、知識情報（ID やパスワード）と所有情報（スマートフォンアプリによるワンタイムパスワードや本人が所有するスマートフォンへの SMS への送信）で認証を行うことが可能です。

CSP 利用サプライヤー向け：多要素認証の設定方法

多要素認証を管理する手順

1. CSP (Coupa Supplier Portal / クーパサプライヤーポータル)にログインをします。
   ログイン URL：https://supplier.coupahost.com
2. ホーム画面右上のユーザー名をクリックし、ドロップダウンメニューから[アカウント設定]＞[セキュリティと多要素認証]を押下します。
3. 認証コードの受信方法に応じて、次のオプションのいずれかを選択し、設定をデフォルトとして設定します。
   ・「支払いの変更のみを有効にする（法人または支払先の変更に必要）」
   ・「アカウントアクセス（ログイン）と支払いの変更の両方を有効にする」
4. 次に認証の方法を「認証アプリ経由」または「SMS 経由」からお選びいただき、有効化を行います。
   ＊CSP の登録時に選択されたオプションがデフォルト値として選択がされています。

   4.1 認証アプリを使用して認証を行う場合は Google Play ストア、または Apple のアプリストアから「Google Authenticator」や「Twilio Authy」などの認証アプリを携帯電話にインストールをしてください。その後 QR コードをスキャンするか、セキュリティキーをコピーして CSP 上に認証コードをご入力ください。

   4.2 携帯電話の SMS を使用して認証を行う場合は、SMS 経由をお選び頂くと、ポップアップ画面が表示されますので、「電話番号」の項目にて国番号を選択いただき、メッセージを受信されたい携帯番号をご入力いただき、［次へ］を押下すると携帯電話に認証コードが届きます。

   4.3 携帯電話がない場合は、ブラウザ拡張機能を用いて多要素認証を実施いただけます。

   I. 該当する拡張機能をブラウザに追加します。

   ・Google Chrome 拡張機能認証ツール。詳細は、「Google Authenticator のインストール」を参照してください。

   ・Mozilla Firefox 拡張機能 オーセンティケーター

   ・Microsoft Edge 拡張機能 オーセンティケータ

   II. オーセンティケータをブラウザに追加します。

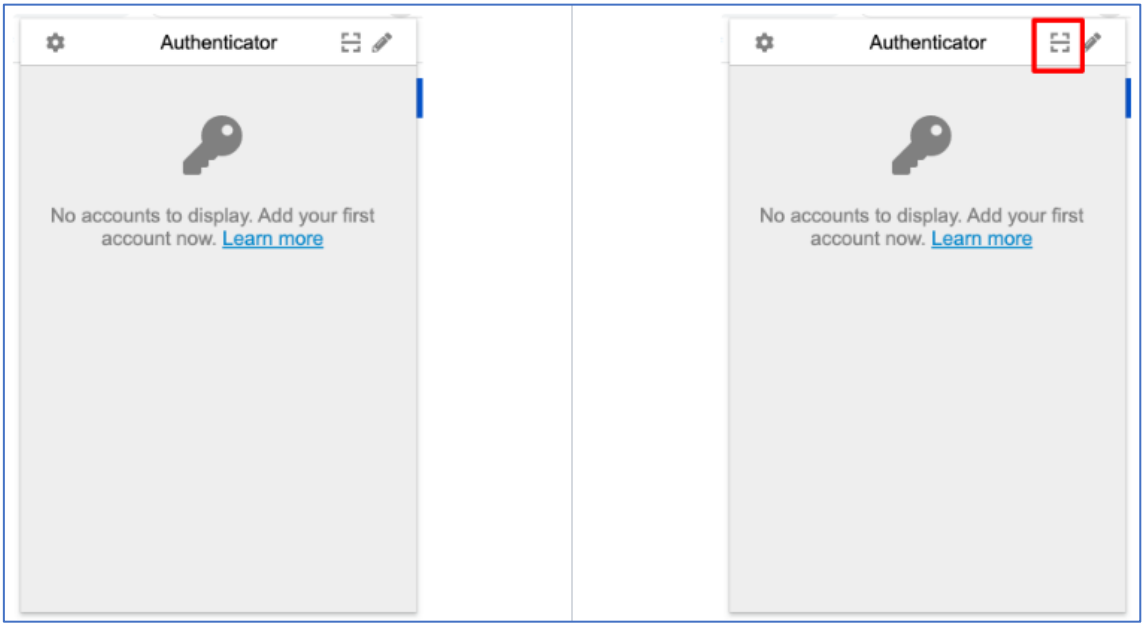
   III. QR コードをスキャンするか、セキュリティキーを CSP ページから認証システムの拡張機能にコピーします。

ブラウザの拡張機能を使用して QR コードをスキャンするには：

I. 該当する拡張機能をダウンロードし、お使いのブラウザにピン留めします。

II. CSP でセキュリティと多要素認証ページに移動し、認証アプリ経由を選択します。[多要素認証アプリ]ポップアップが表示されます。

III. [認証]拡張機能をクリックし、[QR コード]アイコンをクリックします。



IV. 認証ポップアップで QR コードを選択します。

V. スキャンが成功すると、CSP が認証者拡張機能に追加されます。

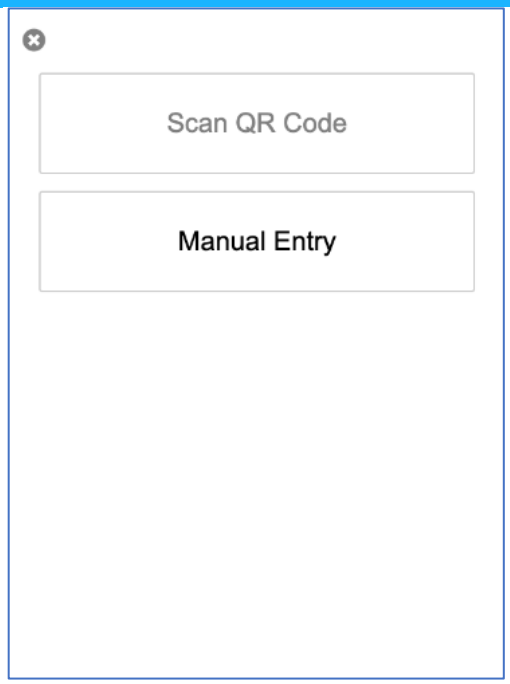
VI. オーセンティケータ拡張機能に表示されているコードをクリックして、CSP にコピー&ペーストします。

ブラウザ拡張機能を使用してセキュリティキーをコピーするには：

I. CSP でセキュリティと多要素認証ページに移動し、認証アプリ経由を選択します。[多要素認証アプリ]ポップアップウィンドウが表示されます。

II. クリックしてセキュリティキーをコピーしますリンクをクリックします。

III. [Authenticator]拡張機能を開きます。



IV. 表示されるポップアップウィンドウで[手動入力]をクリックし、発行者名を入力して、シークレット（セキュリティキー）を貼り付けます。

V. [OK]をクリックし、コードをコピーして CSP に貼り付けます。

バックアップコードはデバイスを紛失した場合、CSP アカウントに再びアクセスするために必要な情報となりますので、［OK］を押下する前にダウンロードまたは印刷をしてください。

多要素認証で困った時の対応手順

サプライヤーからのよくあるお問い合わせ

Coupa のサプライヤー・サポートチームには以下のお問い合わせが寄せられています：

1. バックアップコード・リカバリーコードが送信されていない
2. バックアップコード・リカバリーコードの保存をしていない
3. 認証アプリを削除してしまった
4. 前任者が使用していた携帯電話へアクセスが出来ないため、電話番号の更新ができない
5. バックアップコード・リカバリーコードを使い切ってしまった

多要素認証において、上記またはその他お困りのことがありましたら Coupa のサプライヤー・サポートチームへメールでのご連絡をお願いいたします。

メールアドレス：　supplier@coupa.com

留意事項：

サプライヤー・サポートチームは日本国外のメンバーにより構成されております。
翻訳機能を用いた日本語での返信となりますことを予めご了承ください。

多要素認証の一時的な無効化の手順

バックアップコード・リカバリーコードがお手元に無い等の理由で多要素認証を無効化されたい場合はサプライヤー・サポートチーム（supplier@coupa.com）までご連絡ください。

【サプライヤー・サポートチームへのメールの例】
表題：
Please deactivate CSP 2FA for *abc.xyz@abc.com*

本文：
2 要素認証の設定が有効化されていますが、ログインできないので無効化してください。
無効化して欲しいメールアドレスは、*abc.xyz@abc.com*、です。

※″*abc.xyz@abc.com*″の部分は無効化したいユーザーのメールアドレスに置き換えください。

サポート担当より以下二点のご提出をお願いさせていただきます：

1. サポートチームより申告書が送付されますので、直筆で①申請者様のフルネーム、②ご署名、③日付、と④メールアドレスをご記入いただき、ご登録のメールアドレス（無効化をしたいメールアドレス）からサポートチーム宛に返信をしてください。
2. ご本人様確認を目的として、お問い合わせ主が御社の社員であり、悪意のある第三者ではないことを明示した内容のメールを、ご同僚の方 2 名様より同じドメインのメールアドレスから supplier@coupa.com 宛に送付してください。

詳しい手順につきましてはサプライヤー・サポートがメールでお送りさせていただきますので、メールの指示に従って無効化の作業を実施してください。