フィッシング詐欺対策について

１．フィッシング詐欺とは

実在する個人や企業の送信者を装った「なりすましメール」を送りつけたり、企業の WEB サイトを騙る偽のホームページに誘導してログインを促したり等の手法でユーザ ID やパスワードなどの個人情報を不正に取得しようとする詐欺行為を指します。

２．お客様へのフィッシング詐欺対策のお願い

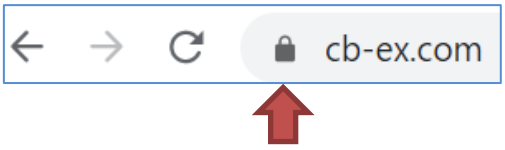
お客様がフィッシング詐欺の被害を受けないようにするため、お客様自身で以下の対策をお願い致します。

（１）WEB サイトの証明書の確認

①ブラウザの URL が表示されている箇所に「鍵マーク」があることを確認します。

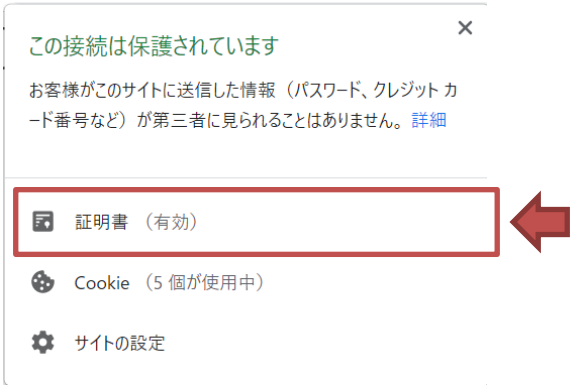
②当社の証明書は「本物のサイトである証明」、及び「企業の実在確認」が含まれるサイバートラスト社の EV-SSL 証明書を利用しておりますので、これが正しい内容であることを確認します（GoogleChrome の場合、鍵マークをクリックし「証明書（有効）」をもう一度クリックすると証明書の詳細が表示されます）。

① URL 欄に鍵マークがあることの確認

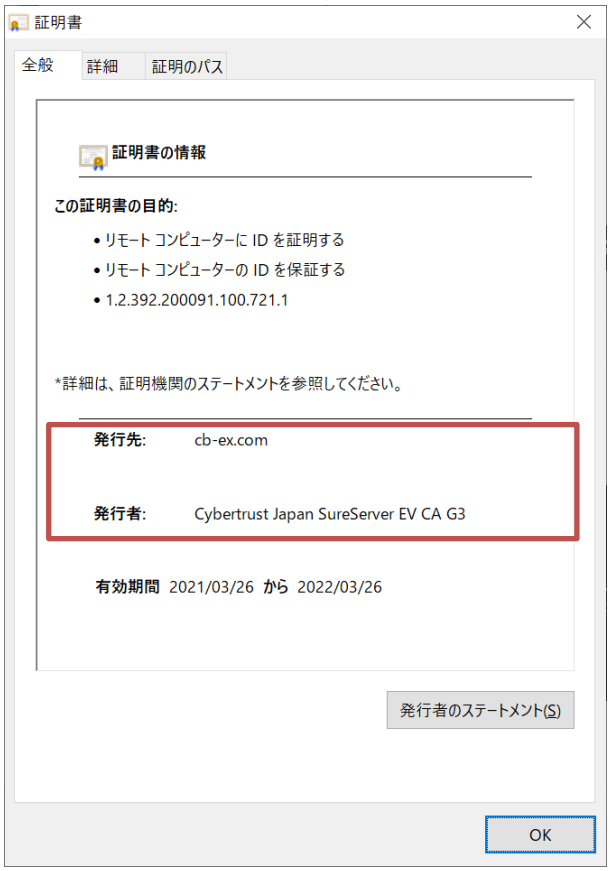


「鍵マークをクリックします。」

② 証明書（有効）の確認



③　証明書の発行者及び発行先の確認



発行先：cb-ex.com
発行者：Cybertrust Japan SureServer EV CA G3
の表記があることを確認します。

（２）不審なメールからのリンクや郵便物はなるべく開かないようにする

お客様ご自身で改めて検索したアドレスや、登録済みのブックマークからアクセスし、不審なメールからのリンクの URL と比較する。フィッシング詐欺のサイトは当社サイトの URL とは異なっているはずです。判断出来ない場合はサイトの運営先に問い合わせをお願い致します。不審なメール内にてお客様のユーザ ID やパスワードの入力を促す場合は特に注意が必要です。

（３）二段階認証

不審なサイトで ID・パスワードを入力してしまった場合を考慮し、二段階認証（SMS 認証、Google 認証など）を導入することで被害を最小限に抑えることが出来ます。

３．フィッシング詐欺対策に関するお問い合わせ

万が一フィッシング詐欺と思われる被害にあわれた場合や不信なメール・郵便物を受け取った場合は、以下までお問い合わせください：

・お問い合わせフォーム：

https://support.coinbook.co.jp/hc/ja/requests/new

以上

2021 年 4 月 22 日

2022 年 10 月 31 日改定