平成29年9月22日

お客さま各位

株式会社 荘内銀行

【重要なお知らせ】インターネットバンキングの不正利用にご注意ください

全国的に、コンピュータウイルスやフィッシングサイトで認証情報（ID・パスワード・メールアドレス・暗証番号）を盗み取ったり、取引にご使用する機器を乗っ取る等、第三者がお客さまになりすまして不正取引を行う金融犯罪が多発しております。
インターネットバンキングを安全にご利用いただくため、下記のセキュリティ対策をお願いいたします。

記

1. ワンタイムパスワード（1回限りの使い捨てパスワード）を積極的にご利用ください

「荘銀ダイレクト」および「わたしの支店」では、ワンタイムパスワードのご利用をおすすめしております。
※パソコンでのお取引には、ワンタイムパスワードもしくはメール通知パスワードのご利用が必須となります。
※スマートフォンでのお取引には、ワンタイムパスワードのご利用が必須となります。メール通知パスワードはご利用できません。

【 ワンタイムパスワードをご利用の場合 】
MITB（Man In The Browser：マン・イン・ザ・ブラウザ）攻撃による被害を防止するため、あわせてソフトウェアトークン取引認証もご利用ください。ご利用の際は、ワンタイムパスワードアプリに表示される内容を必ずご確認のうえ、お取引をお願いします。

《 ソフトウェアトークン取引認証とは 》
スマートフォンにインストールしたワンタイムパスワードアプリで、取引内容の確認・承認ができる機能です。

《 MITB（Man In The Browser：マン・イン・ザ・ブラウザ）とは 》
パソコン等に感染したウイルスが、インターネットとの通信を傍受し、取引内容の一部を改ざんするサイバー攻撃のことです。

【 メール通知パスワードをご利用の場合 】
パソコンの乗っ取りによる不正利用防止のため、メール通知パスワードの送信先には、お取引に使うパソコンやフリーメール以外のメールアドレス（別のパソコン、携帯電話・スマートフォン等）を設定してください。

なお、「荘銀ビジネスダイレクト」につきましては、従来のワンタイムパスワードよりセキュリティが強化されたトランザクション認証を提供しております。ご利用の際は、トークン機器に表示される内容を必ずご確認のうえ、お取引をお願いします。

2. ID・パスワード等の取扱いおよび管理にご注意ください

電話で金融機関の職員を名乗り、ワンタイムパスワード等を聞き出して、金銭を不正送金する詐欺が発生しております。
ID・パスワード等は、厳重な管理を行い、決して第三者に教えないでください。当行行員・銀行協会職員・警察官等が、ID・パスワード等をおたずねすることは絶対にありません。

・類推されやすいID・パスワード等のご使用は避け、定期的に変更を行ってください。
・漏えい防止のため、他サービスで同一ID・パスワードを使い回さないようにしてください。
・お客さまご自身が所有・管理していない機器や、ネットカフェ・FREE Wi-Fi等の不特定多数の人が使用するパソコン・ネットワークではご利用しないでください。

3. 電子証明書方式をご利用ください

「荘銀ビジネスダイレクト」では、ログイン時の認証方式として、ID・パスワード方式より安全性の高い電子証明書方式を提供しております。

《 電子証明書方式とは 》

第三者機関である認証局が発行した、当行の電子証明書をお客さまのパソコンにインストールしていただくことで、「荘銀ビジネスダイレクト」にログイン可能なパソコンを特定できる認証方式です。電子証明書がインストールされたパソコンからしかログインできないため、外部からの不正利用を防止することができます。

4. セキュリティ対策ソフト「PhishWall プレミアム」をご利用ください

「PhishWall（フィッシュウォール）プレミアム」は、アクセスしたサイトが偽装されていないかを確認できるフィッシング対策機能や、偽の画面を表示してパスワード等を盗み取ろうとするMITB（Man In The Browser：マン・イン・ザ・ブラウザ）攻撃を検知・無効化する機能を搭載したソフトウェアです。無償で提供しておりますので、ぜひご利用ください。

5. 振込限度額は可能な限り低く設定してください

不正送金された場合の被害を最小限に抑えるため、1日あたりの振込限度額を、必要な範囲で可能な限り低く設定してください。

なお、「荘銀ダイレクト」および「わたしの支店」では、平成29年2月20日（月）より、ワンタイムパスワードをご利用されていないお客さま（メール通知パスワードをご利用のお客さま）の「1日あたりの振込・振替限度額」に設定できる金額上限を10万円としております。

6. ログイン履歴・取引履歴をご確認ください

不審なログイン履歴や取引履歴がないか、こまめにご確認ください。

7. 携帯電話やスマートフォンのメールアドレスをご登録ください

インターネットバンキングでは、振込等の取引時に、取引通知メールを送信しております。
携帯電話やスマートフォン等、お客さまが常に持ち歩く機器のメールアドレスを登録していただき、不審なお取引がないかこまめにご確認ください。

8. OS・ブラウザ等は最新の状態でご利用ください

OSやブラウザ等の各種ソフトウェアは、常に最新の状態に更新してご利用ください。

9. セキュリティ対策ソフトを必ず導入してください

お取引にご使用する機器には、必ずセキュリティ対策ソフトを導入してください。また、常に最新の状態に更新してご利用ください。

10. 不正なポップアップ画面を表示させて情報を盗み取ろうとする犯罪にご注意ください

当行では、インターネットバンキングのログイン後にポップアップ画面を表示して、ID・パスワードや乱数表等の入力を求めることはございません。
このような事象は、ウイルス感染した場合に発生する可能性がございますので、OS・ブラウザやセキュリティ対策ソフトは最新の状態でご利用ください。

11. 不審なメールにご注意ください

金融機関を装い、インターネットバンキングの取引通知メールにウイルス感染させるファイルを添付する等の不審なメールが確認されております。
当行では、インターネットバンキングの取引通知メールにファイルを添付することはございません。
身に覚えのない不審なメールは絶対に開かず、速やかに削除してください。

12. 当行ホームページを装った偽サイトにご注意ください

当行を含む、多数の国内ホームページを装ったフィッシングサイトが確認されております。偽サイトには、決してアクセスしないようご注意ください。ご利用の際は、アドレス（URL）欄をご確認ください。
通常、アドレス（URL）は、ブラウザのウィンドウや画面上部に「http://www～」や「https://www～」から始まる文字で表示されています。「http://」部分は省略される場合もあります。

ブラウザのアドレス欄の先頭部分と、ご利用中のサービスのアドレス（以下表をご覧ください）が完全に一致していることをご確認ください。

サービス名・サイト名	アドレス（URL）
荘内銀行ホームページ	http://www.shonai.co.jp/
「SHOGIN Web Branch“わたしの支店”」 荘銀バンキングサービス「荘銀ダイレクト」	https://www.parasol.anser.ne.jp/
法人向け荘銀インターネットEBサービス「荘銀ビジネスダイレクト」	https://www.bizsol.anser.ne.jp/
インターネット投資信託サービス「荘銀投信ダイレクト」	https://prod.sonar-ic.jp/
新卒採用サイト「荘内銀行メンバーズサイト」	https://job.axol.jp/

※フィッシングサイトのアドレス（URL）には、本物と間違えやすい文字が使われますので、ご注意ください。

上記以外のアドレス（URL）のサイトにつきましては、当行とは一切関係がなく、お問い合わせいただきましても適切な対応やご案内ができかねますので、ご了承ください。

以上

身に覚えのないお取引がある場合や、不審なメール・サイト等を発見された場合は、直ちにダイレクトサポートセンター（TEL 0120-61-4071(1#) 平日9:00-19:00）へお問い合わせくださいますよう、お願い申し上げます。