

セキュリティについて

最新の暗号化技術

最新の暗号化技術であるSSL (Secure Socket Layer) 128bitを導入し、高いレベルの安全性を確保しています。

複数の情報から本人確認を実施

お取引の際には、契約者番号、暗証番号、確認番号、確認暗証番号を使用し、ご利用されるお客さまの本人確認を行っております。

※契約者番号、確認番号は契約者カードに記載されています。また、確認番号は乱数表方式のワンタイムパスワードとなっております。

※暗証番号は、当初、お客さまが商工中金ダイレクト申込書などにご記入いただいた4桁の数字です(お客さまご自身の機器操作でご変更できません)。

※確認暗証番号は、お客さまがインターネットバンキングで初期登録時に、ご登録いただいた6桁～12桁の英数字です(お客さまご自身の機器操作でご変更できます)。

前回ご利用日時を表示

インターネットバンキングにログイン後のお客さま情報画面に、直近3回のログイン日時を表示しますので、第三者による不正アクセスのチェックが可能です。

ログインの際には、毎回確認する習慣をつけてください。

お取引結果の通知

お振込や定期預金のお預け入れなどの予約受付時や実行時、Eメールアドレス変更時には、Eメール通知を行いますので、Eメールアドレスは必ず最新のE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、モバイルバンキングで各々登録を行ってください)。

ソフトウェアキーボード

キーボード操作から情報を不正に盗み取るスパイウェア対策として、画面キーボードを導入しています。

スパイウェアに対するセキュリティ対策として、暗証番号や確認番号などの入力をパソコンの画面上に表示するボタンをマウスでクリックすることにより入力していただく機能です。キーボードの操作履歴がパソコンに残らないため、パソコンのキーボード情報を盗み、インターネット経由で第三者に送信するキーロガー型のスパイウェアに対し有効です。

暗証番号などの誤入力によるロック

インターネットバンキングおよびモバイルバンキングで暗証番号や確認番号、確認暗証番号を一定回数以上誤って入力するとロックがかかります。ご利用できなくなります。

※テレホンバンキングにおいて、暗証番号などを一定回数以上続けて誤入力した場合は契約が解除されますのでご注意ください。

※ロックの解除は別途、書面によるお手続きが必要です。

自動タイムアウト(自動ログアウト)機能

インターネットバンキングにログインしたまま離席した場合など、一定時間操作がなかった場合には、自動的にログアウトし、お取引を終了させていただきます。これにより、第三者の不正利用を防ぐよう配慮しています。

振込限度額の設定

インターネットバンキング、モバイルバンキングの各々で振込限度額を上限500万円以内で変更できます。

※限度額の初期値は500万円となっておりますので、お客さま情報(その他)変更画面より変更してください。

フィッシング対策

フィッシング詐欺対策として、当金庫ではフィッシング対策ソフト「PhishWall(フィッシュウォール)」および「EV SSL証明書」を導入しております。

詳しくはご利用にあたっての留意事項42ページをご覧ください。

ご利用にあたっての留意事項

セキュリティ(安全にご利用いただくために)

暗証番号などの管理について

商工中金ダイレクトの「暗証番号」・「確認番号」・「確認暗証番号」は、印章・通帳・証書・キャッシュカードなどにかわる非常に大切なものです。以下の点にご注意のうえ、お客さまご自身で厳重な管理をおこなってください。

- 暗証番号、確認暗証番号は、「インターネットバンキング」または「モバイルバンキング」から、随時ご変更ください。
- 暗証番号は、「テレホンバンキング」と、「インターネットバンキング・モバイルバンキング」で別々に変更してください。
- 暗証番号、確認番号、確認暗証番号(以下「暗証番号など」といいます)は、絶対に第三者に教えないでください。当金庫職員や警察官などであっても、お客さまにこれらの「暗証番号など」をおたずねすることは絶対にありません。
- 「暗証番号など」は、第三者の目に容易に触れるところや運転免許証・通帳・キャッシュカード・契約者カードなど、類推されるおそれのあるものには絶対に書き留めないでください。
- 「暗証番号など」は、テキストファイル・ワード・エクセルなどに記載して、パソコンに保存しないでください(特にファイル交換・共有ソフトを利用している場合は絶対に保存しないでください)。なお、ブラウザには一度記録された「暗証番号など」をブラウザに自動的に入力する機能(「オートコンプリート」機能、「自動入力フォーム」等)がありますが、セキュリティ上、これらの機能をご利用できないようブラウザの設定を行うようお願いいたします(ブラウザの設定方法は各ブラウザのヘルプ等をご参照ください)。
- 「暗証番号など」をパソコンや携帯電話などからご入力になる場合、テレホンバンキングで暗証番号を公衆電話などからご入力になる場合、第三者に知られないようにしてください。
- 「暗証番号など」を第三者に知られてしまった、もしくは知られてしまったと思われるときは、ただちにインターネットバンキングまたはモバイルバンキングから、お客さまご自身で「暗証番号など(確認番号除く)」の変更手続きをおこなってください。契約者カードを紛失もしくは盗難されてしまった(暗証番号を第三者に知られてしまった、もしくは知られてしまったと思われるときを含む)ときは、ただちに、商工中金ダイレクトバンキングセンターやお取引店、夜間等緊急連絡先のいずれかに、それぞれの受付時間内(P.49)にご連絡ください。
- お客さまご自身が所有・管理する端末以外からやむを得ず操作された場合は、操作後速やかに暗証番号、確認暗証番号を変更してください。
- 他のサイトで利用されている暗証番号、確認暗証番号は使用しないことをお勧めします。
- 他人に推測されやすい数字など(生年月日、電話番号、住所、1111、AAAAAAAなどの同じ英数字)を暗証番号、確認暗証番号に使用しないでください。

- インターネットバンキングのご利用時に契約者番号・暗証番号などのご入力の際は、アドレスバーのURLを必ずご確認のうえ、正當な画面へアクセスしているかご確認ください。

インターネットバンキングのログイン画面(操作画面) URL
<https://www.ics12.finemax.net/2004schukin/BankContents/CTLOGO.html>
 半角英大文字(オー) 
 半角数字(ゼロ) 

ファイル交換・共有ソフトのご利用にご注意ください!

最近、各地の金融機関において、ファイル交換・共有ソフト(ウィルスではないため、ウィルス対策ソフトでは検知できません)を使用しているお客さまが、暗証番号などをテキストファイル・ワード・エクセルなどに記載して、パソコンに保存していたため、暗証番号などが不正に盗まれ、お客さまの口座から身に覚えのない振込出金がかかるという事件が発生しています。

以下の点にご注意のうえ、お客さまご自身で厳重な管理をおこなってください。

1. ファイル交換・共有ソフトを利用されているパソコンでは、インターネットバンキングをご利用にならないでください。
2. インターネットバンキングを利用されているパソコンからはファイル交換・共有ソフトの削除をお勧めします。

インターネットバンキングのご利用場所にご注意ください!

インターネットカフェなど、ご自身が所有・管理するパソコン以外からご利用される場合、パソコンに暗証番号を盗み見るソフトが仕掛けられ、暗証番号が漏洩する危険があります。

インターネットバンキングをご利用のお客さまは、以下の点にご注意ください。

1. インターネットカフェなど、不特定多数が利用するパソコンではインターネットバンキングを利用しないでください。
2. お客さまご自身が所有・管理するパソコン以外からやむを得ず操作する場合は、ソフトウェアキーボードを必ずご利用になり、事後、お客さまが所有・管理するパソコンから速やかに暗証番号などを変更してください。

スパイウェアなどのウィルスへの対策と最新版へのアップデートをお願いします！

最近、各地の金融機関において、スパイウェアと呼ばれるソフトなどにより、お客さまのパソコンから暗証番号などが不正に盗まれ、お客さまの口座から身に覚えのない振込出金がされるという事件が発生しています。インターネットバンキングご利用のお客さまは、以下の点にご注意ください。

1. ウィルス対策ソフトやファイアウォールを必ずご利用ください。
2. ウィルス対策ソフト、オペレーションシステム(OS)、ブラウザ(インターネット閲覧用ソフト)は常に最新版にアップデートしてください。
3. 心あたりのないEメールに添付されているファイルを開封したり、不審なサイトにアクセスしないでください(ウィルスに感染する可能性があります)。

※ウィルス対策ソフトは、100%安全が保証されるものではありませんが、新種のウィルス登場から数時間から数日で対策プログラムが公表される場合が一般的であり、最新版へ定期的にアップデートすることでウィルスが侵入するリスクが軽減されます。

▶▶▶ スパイウェアとは？

他人のコンピュータに入り込んで、そのユーザーの個人情報や暗証番号などを利用者が気付かないうちに収集して、その結果をインターネット経由で送信してしまう不正なソフト。以下の手口でパソコンに侵入する場合があります。

- Eメールの添付ファイルの開封時
- フリーソフトをダウンロード時
- ファイル交換ソフト利用時
- 不審なサイト接続時

他の金融機関で実際おこなわれた犯罪手口

1. 感染経路はEメールに添付されているファイル。
2. Eメールに添付されたファイルを解凍・実行すると、インターネットバンキングなどにアクセスした際に契約者番号・暗証番号などを特定のアドレス(第三者)に自動的に送信するスパイウェアが作成されてしまう。

※この事象で発見されたスパイウェア(TSPY_BANCOS.ANM)では、「system.exe」というファイルが作成され、パソコンのCドライブ真下に「system.exe」あるいは「system」というファイルがある場合はスパイウェアである可能性があるのでご注意ください。

ソフトの設定・ダウンロードにご注意ください！

不審なサイトから不審なソフトをダウンロードする場合、ウィルスに感染する危険があります。また、無線LANなどのセキュリティ機能の設定ミスなどでも暗証番号などが漏洩する危険があります。インターネットバンキングご利用のお客さまは、以下の点にご注意ください。

1. 不審なサイトにアクセスしたり、不審なサイトからソフトをダウンロードしないでください(ウィルスに感染する可能性があります)。
2. パソコンに搭載しているOS(Windows、MacOSなど)やブラウザ(Internet Explorer)は、公式サイトを通じて提供されるセキュリティ面が強化された最新の修正プログラムをご利用ください。
3. 心あたりのないEメールに添付されているファイルを開封したり、不審なサイトにアクセスしないでください(ウィルスに感染する可能性があります)。
4. 無線LANをご利用の方は、セキュリティ機能の設定を必ずおこなってください。

※ウィルス対策ソフトは、100%安全が保証されるものではありませんが、新種のウィルス登場から数時間から数日で対策プログラムが公表される場合が一般的であり、最新版へ定期的にアップデートすることでウィルスが侵入するリスクが軽減されます。

Eメール詐欺にご注意ください！

心あたりのないEメールに添付されているファイルを開封したり、心あたりのないEメールに記載されているURLにアクセスしたりするとウィルスに感染する危険があります。また、虚偽のEメールを使用するフィッシング(phishing)詐欺により暗証番号などが漏洩する危険があります。インターネットバンキングご利用のお客さまは、以下の点にご注意ください。

1. 心あたりのないEメールに添付されているファイルを開封したり、心あたりのないEメールに記載されているサイトにアクセスしないでください(ウィルスに感染する可能性がありますので開封せずEメールごと削除することをお勧めします)。
2. Eメール経由でサイトにアクセスした場合、個人情報や暗証番号などの入力を求められても絶対に入力しないでください(当金庫では、Eメール経由でサイトに誘導して個人情報や暗証番号などを入力させることは絶対にありません)。

当金庫からお取引の結果を送信するEメールアドレス
schukin@finemax.net

※その他当金庫よりキャンペーンのご案内などをEメールで行う場合がございます。インターネットバンキングの操作画面からEメールの配信要否を設定できます(ただし、サービスの一時休止などの大事なお知らせはご契約されている皆さまに配信いたします)。

キャンペーンのご案内などのEメールアドレス
schukininfo@ib.shokochukin.co.jp

3. 当金庫のホームページ閲覧の際は、アドレスバーのURLを必ずご確認ください。

(参考)当金庫ホームページ

<http://www.shokochukin.co.jp/>

フィッシング(phishing)詐欺とは?

金融機関やオンラインショッピング事業者などを装い、偽りの情報を記載したEメールを送りつけ、本物と酷似したWebサイト(フィッシングサイト)へ誘導し、氏名、住所、預金口座番号や、クレジットカード番号、暗証番号などを入力させ、不正に個人情報を入手しようとする行為。

フィッシング詐欺 防止対策1

「PhishWall(フィッシュウォール)」を導入しています。

PhishWall(フィッシュウォール)とは、株式会社セキュアブレインの提供するフィッシング対策ソフトです(無償でインストールできます)。ブラウザのツールバーに表示されたシグナルにより、Webサイトが本物が偽造されたものであるかを確認することができます。ソフトをインストールすると、ブラウザに以下のようなツールバーが表示されます。

セキュリティ対策としてご利用をおすすめします。



商工中金ホームページ(ホーム画面)のアドレス
<http://www.shokochukin.co.jp>

商工中金ダイレクトログインページのアドレス
<https://www.ics12.finemax.net/2004schukin/BankContents/CTLOGOA.html>

フィッシング詐欺 防止対策2

「EV SSL証明書」を導入しています。

▶EV SSL証明書とは?

EV SSL(Extended Validation SSL)証明書とはウェブサイトの証明書のことで、

以下の対応ブラウザを利用しているお客さまがEV SSL証明書で保護されている当金庫のインターネットバンキングにログインすると、アドレスバーが緑色に変わり、アドレスバーに表示されたURLの横に、「ウェブサイトを運営する組織名」と「SSL証明書を発行した認証局名」が表示されます。

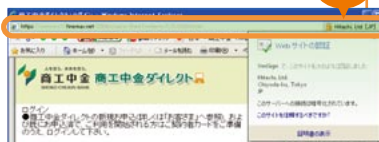
この緑色のバーは、EV SSL証明書が、組織の実在性、そのドメイン名を使用する権利を組織が保有しているかなどを検証したうえで、正式に発行されたものであることを意味しています。

▶対応ブラウザ

インターネットバンキングでご利用が可能なブラウザのうち、以下のブラウザが対応しています。

- Internet Explorer7以降
- Firefox3.5以降
- Safari4.0以降

※Internet Explorer6では、アドレスバーは緑色にはならず、鍵マークのみが表示されます。



Eメールアドレスの設定などにご注意ください!

万一、暗証番号などの漏洩により不正利用された場合でも、即時に気付いた場合、被害を最小限に食い止められる場合があります。インターネットバンキング・モバイルバンキングご利用のお客さまは、以下の点にご注意ください。

- 1.お振込や定期預金のお預け入れなどの予約受付時や実行時、Eメールアドレス変更時には、Eメール通知を行いますので、Eメールアドレスは必ず最新のものをご登録ください。Eメールアドレスの登録は、インターネットバンキング、モバイルバンキングでそれぞれ行ってください(インターネットバンキングで登録を行っても、モバイルバンキングには反映されません)。
- 2.Eメールアドレスは、携帯電話で利用しているEメールアドレスも登録できます。
- 3.振込限度額は、インターネットバンキング、モバイルバンキング、それぞれ適切な限度額を設定してください。
- 4.心あたりのないEメールアドレスの変更、振込限度額の変更、振込受付のEメール通知を受けた場合、即時に利用停止登録を行ってください。

銀行を偽装して郵送される「CD-ROM」にご注意ください!

他の金融機関において、「法人向けインターネットバンキング」ご利用のお客さま向けに当該金融機関を偽装した「CD-ROM」が送付され、そのお客さまがその「CD-ROM」をパソコンにインストールしたところ、ウイルス(スパイウェア)に感染して、暗証番号などが盗み取られて、お客さまの口座から身に覚えのない振込出金がされるといふ事件が発生しています。インターネットバンキングご利用のお客さまは、以下の点にご注意ください。

- 1.当金庫では、「商工中金ダイレクト」をご利用のお客さまに、「CD-ROM」でソフトウェアをお送りすることは一切行っておりません。万一、当金庫名で「CD-ROM」が送付された場合は、絶対にパソコンに挿入することのないようご注意ください。
- 2.その他不審な「CD-ROM」をパソコンに挿入することのないようご注意ください。
- 3.スパイウェアなどのウイルスへの対策と最新版へのアップデートを必ず行ってください。

還付金詐欺にご注意ください!

最近、他の金融機関において、以下のような手口で還付金詐欺が発生しています。

- 税務署や保険会社などを名乗り、「還付金を返金します。お金を振り込むための用紙を送付するので銀行に返信してください。」との電話があり、後日インターネットバンキングの利用申込書が送付されます。
- 記名・押印後、銀行に返送した場合、インターネットバンキング契約手続き完了後、銀行から暗証番号などが記載された利用開始案内書が届くが、その頃再度、「還付の手続きをするので、書類に記載されている暗証番号やパスワードなどを確認のため読みあげてください。」と電話がある。
- ここで「暗証番号など」を教えてしまうと、インターネットバンキングで本人確認をおこなうとともに振り込みがおこなえる重要な情報であるため、口座から不正に資金が引き出されてしまいます。

還付金詐欺等の被害にあわないため、以下の点にご注意のうえ、お客さまご自身で厳重な管理をおこなってください。

1. 商工中金ダイレクトのお申し込みによって、税金・保険金等が還付されることはありません。
2. 当金庫職員や警察官、税務署職員などであっても、電話でキャッシュカードや商工中金ダイレクトなどで利用する「暗証番号など」をおたずねすることは絶対にありません。「暗証番号など」の重要情報は絶対に第三者に教えないでください。
3. 上記のような利用申込書が公的機関から送付されてきても、絶対に返送しないでください。
4. 申し込みの覚えのない「利用開始案内」などが郵送された場合、ただちに商工中金ダイレクトバンキングセンターまたは、お取引店までおたずねください。

その他「架空請求」などのネット犯罪にご注意ください!

インターネットバンキングを不正利用する金融犯罪以外にも、インターネット上にはさまざまな犯罪があります。例えばホームページを閲覧しただけで不正な請求をされる「架空請求」の被害が各地で発生しています。インターネットバンキングご利用のお客さまに限らずインターネットをご利用の場合、以下の点にご注意ください。

1. **利用していなければ払わない**
身に覚えのない請求なら支払う必要はありません。
2. **消費者センターへ相談する**
不審に思った場合は、迷わずお近くの消費生活センターなどの窓口相談する。
3. **個人情報は絶対に知らせない**
安易に個人情報(自宅の住所、電話番号、勤務先など)を絶対に教えないでください。
4. **証拠は保管しておく**
請求のハガキ・封書・メールなど証拠となるものは保管しておきましょう。
5. **警察へ届出をおこなう**
悪質な請求は警察にも届け出ましょう。

▶ 架空請求とは?

架空請求とは、はがきや封書、電報のほかパソコンのメールや携帯電話を使い、有料番組サイト利用料金、恋人紹介事業の事務手数料、民法指定消費料金、債権など全く根拠のない請求をする文書が届き、現金の振り込みを要求する行為です。

請求の内容は、「入金がない場合には自宅、勤務先へ回収に向く」「回収員が自宅へ向く」「勤務先を調査」「送料の差押え」「強制執行」「信用情報機関に登録」など脅迫まがいのものが多く、ほとんどの場合、利用したとされる番組名、日時、利用時間など、請求明細が示されていません。あるいは過去に自分が使った別事業者の請求と勘違いしたり、家族が使ったと思いこんだりして、支払ってしまうなど、勘違いや関わりになりたくない気持ちなどに付け込む手口です。

このような請求をする業者が「商工中金」などと名乗っていても、当金庫とは一切関係ありません。また、当金庫ではこのようなご連絡は差し上げておりませんのでご注意ください。

その他の留意事項

- ご利用は、総合口座をお持ちの個人のお客さまご本人に限らせていただきます。
- ご利用は、お客さまご本人名義の口座となります。
- 既に商工中金テレホンバンキングをご契約されている方が、インターネット/モバイルバンキングを追加でお申し込みいただく場合、新しい契約者カードは送付いたしませんので、お手持ちの契約者カードをそのままご利用ください。
- 定期預金のお預入れ、お振込(お振替)は総合口座普通預金の支払可能残高までお取引できます。支払可能残高は、残高に当座貸越でお借り入れできる額を加えたものです(貸越利息が発生します)。詳しくは総合口座取引規定をご覧ください。
- 以下のような場合には、ご契約を解除させていただきますのでご注意ください(詳しくは「商工中金ダイレクト利用規定」をご確認ください)。
 - 総合口座を解約した場合
 - 相続が発生した場合
 - お届先不明などにより、当金庫からご郵送した文書などが返送された場合
 - 支払停止、または破産、再生手続開始の申立があった場合
 - テレホンバンキングにおいて、暗証番号などを一定回数以上続けて誤入力した場合

- 「お取引結果通知」を受信するEメールアドレスは常時利用しているEメールアドレスを設定してください。
- Eメールアドレスを変更された場合は、必ず「Eメールアドレスの設定」から最新のEメールアドレスをご登録ください(お手続きされないと「お取引結果通知」が送信されません)。
- ご利用にあたっては、必ず商工中金ホームページ(<http://www.shokochukin.co.jp/>)*からアクセスしてください。また、当金庫ホームページ上には、最新時点のサービス内容や、セキュリティ情報、お客さまにご注意していただきたい事項を掲載しておりますので、ご利用前にご確認くださいようお願いいたします。

*商工中金ダイレクト サービスのご案内ページ
<http://www.shokochukin.co.jp/directbanking/index.html>

以上記載されている社名および商品名は、各社の登録商標または商標です。

お困りの時は〈Q&A〉

Q1 携帯電話の機種変更を行いたいのです。

A1 旧携帯電話のサービス利用登録(マイメニュー登録)を解除後、新携帯電話のサービス利用登録(マイメニュー登録)を行ってください。

Q2 振込、振替を行う場合の振込先名義人の入力方法を教えてください。

A2 **ご注意ください**
振込先名義人名は、下記【ご使用可能文字】を参考に正しく入力してください。誤って入力した場合、振込先金融機関で入金処理を行えず、資金が返却される場合などがございますのでご注意ください。

※申し訳ございませんが、当金庫では振込でネームバック機能(銀行名、支店名、口座番号を入力すると自動的に受取人名が表示される機能)をご利用いただけませんので、ご容赦ください。

【ご使用可能文字】

- お振込、お振替先の名義人名は、全て半角(大文字)でご入力ください。
- スペースは1文字としてカウントします。
- ひらがな・漢字や全角カナはご使用いただけません。
- お受取人名が個人の場合は、姓と名の間にスペースを1つ入れてください。
- お受取人名が法人の場合は、略語をご使用ください。

半角カナ (大文字)	アイエオ カクケコ サシセリ タチツテ ナニネノ	ハヒフヘホ マミムメモ ヤユヨ ラリルレロ ワヲン	ガギグゲゴ ザズゼゾ ダヂヅデド バビブベボ パピプペポ
半角数字	0123456789		
アルファベット (半角大文字)	ABCDEFGHIJKLMNOPQRSTUVWXYZ		
記号	¥ , .「 」 () / -		

【受取人名に「株式会社」などを入力する場合の入力方法】

- 受取人名に「株式会社」などを入力される場合は、次の略語をご使用ください。
- 略語をご利用になる際は、次のルールでご利用ください。

先頭に使うとき 株式会社商工中金 ⇒ カ)シヨウコウチュウキン

途中に使うとき 商工中金株式会社九段営業所 ⇒ シヨウコウチュウキン(カ)クワン(エイ)

末尾に使うとき 商工中金株式会社 ⇒ シヨウコウチュウキン(カ)

正式名称	略語	正式名称	略語
株式会社	カ	学校法人	ガク
有限会社	ユ	社会福祉法人	フク
合名会社	メ	相互会社	ソ
合資会社	シ	特定非営利活動法人	トクヒ
医療法人	イ	独立行政法人	ドク
医療法人社団	イ	弁護士法人	ベン
医療法人財団	イ	有限責任中間法人	チュウ
財団法人	ザイ	無限責任中間法人	チュウ
社団法人	シヤ	営業所	エイ
宗教法人	シユウ	出張所	シユツ

Q3 暗証番号、確認暗証番号を忘れてしまったのですが？

A3 「暗証番号」は、「商工中金ダイレクト申込書」をご提出していただき、契約者カード再発行のお手続きを行うことで、再度、暗証番号を登録し直すことができます。
「確認暗証番号」は別途、当金庫所定の書面をご提出ください。書面の受付後、確認暗証番号を初期化(消去)します。お客さまは初期化終了後、改めて確認暗証番号を登録してください。

Q4 利用する時に暗証番号などの入力を間違えるとどうなるのですか？

A4 一定回数以上累計で暗証番号、確認番号、確認暗証番号のご入力を間違えると自動的にご利用を停止します(ロックがかかります)。

ご利用の再開には、当金庫所定の書面をご提出ください。書面の受付後、ロックを解除します。

なお、暗証番号、確認暗証番号を失念されている場合は、Q3のお手続きを行ってください。

また、契約者カードの紛失などにより確認番号が分からない場合は、Q7の契約者カードの紛失のお手続きを行ってください。

Q5 暗証番号、確認暗証番号を第三者に知られてしまったおそれのある場合はどうすればよいですか？

A5 暗証番号、確認暗証番号のいずれかを第三者に知られてしまったおそれのある場合は、インターネットバンキング・モバイルバンキングでただちに「暗証番号の変更」、「確認暗証番号の変更」を行ったうえで、商工中金ダイレクトバンキングセンター（受付時間：平日【銀行営業日】9：00～19：00）にご連絡ください。それ以外の時間帯は、お取引店または夜間等緊急連絡先へそれぞれの受付時間内（P.49）にご連絡ください。

Q6 「契約者カード」の再発行はできますか？

A6 契約者カードの紛失や破損・汚損、暗証番号の失念時などは「商工中金ダイレクト申込書」をご提出していただき、「契約者カード」の再発行手続きを行います。

Q7 「契約者カード」を紛失または盗難されてしまったのですがどうすればいいのですか？

A7 契約者カードを紛失または盗難されてしまった場合は、ただちに、商工中金ダイレクトバンキングセンター（受付時間：平日【銀行営業日】9：00～19：00）にご連絡ください。それ以外の時間帯は、お取引店または夜間等緊急連絡先へご連絡ください（P.49）。

なお、「契約者番号と、インターネットバンキング・モバイルバンキングの暗証番号（モバイルバンキングは加えて確認暗証番号）」または「総合口座普通預金口座番号と、インターネットバンキング・モバイルバンキングの暗証番号」のいずれかが分かる場合は、お客さまご自身でサービスの「利用停止」を行うこともできます。

【利用停止を行う場合のご注意事項】

インターネットバンキング、モバイルバンキングのうち、一方だけ利用停止を行っても、他方には反映されませんので、インターネットバンキング、モバイルバンキング各々で、利用停止の登録を行ってください。

また、利用停止を行うと、予約受付を行っていたお取引や処理中のお取引が全て無効となります。利用停止を解除する場合は、別途書面によるお手続きが必要となります。

ご連絡や各種お手続きの問い合わせ先

- 商工中金ダイレクトバンキングセンター
平日（銀行営業日）9：00～19：00
フリーダイヤル
0120-064-056（契約者専用）または
0120-299-233（一般用）

契約者カード紛失・盗難時など緊急時のご連絡先

- 商工中金ダイレクトバンキングセンター
フリーダイヤル **0120-064-056**（契約者専用）
フリーダイヤル **0120-299-233**（一般用）
受付時間：平日（銀行営業日）の9：00～19：00
- お取引店までお問い合わせください。
受付時間：平日（銀行営業日）の8：40～17：00
- 夜間等緊急連絡先（キャッシュカード管理センター※）
※受付窓口は、時間帯により、「キャッシュカード管理センター」または「カード紛失共同受付センター」となります。
フリーダイヤル **0120-155-215**
受付時間：平日（銀行営業日）の8：40～17：00 以外の時間帯
土・日曜、祝日、振替休日、銀行休業日は24時間

当金庫ホームページの障害時には以下のアドレスを直接入力することで、インターネットバンキングをご利用いただけます。

<https://www.ics12.finemax.net/2004schukin/BankContents/CTLOG0A.html>

半角英大文字（オー）
半角数字（ゼロ）