

【重要】Pay-easy収納サービスのご利用限度額を引き下げます

～Pay-easy（ペイジー）収納サービスを利用した不正送金にご注意ください～

インターネットバンキングの Pay-easy（ペイジー）収納サービスを悪用し、Amazon 等のチャージタイプのギフト券を購入されてしまう不正送金被害が、複数の金融機関において発生しております。

これは Pay-easy の機能を使った新手的な不正送金手口で、日ごろ同機能を使わない方でも、高額な不正送金被害にあう可能性がございます。

そのため、弊行ではお客さまの大切な資産をお守りすることを最優先するため、Pay-easy 収納サービスのご利用限度額を、平成28年12月10日(土)から50万円に引き下げさせていただきます。何卒ご理解いただきますようお願い申し上げます。

なお、ワンタイムパスワードをご利用いただく場合は、Pay-easy 収納サービスは従来通り1億円までご利用いただけます。

ワンタイムパスワードのご利用を希望される場合は、お取引店、または下記お問い合わせ先までご連絡いただけますようお願い申し上げます。

Pay-easy（ペイジー）収納サービスのご利用限度額の変更

平成28年12月10日(土)～

現在	変更後
1億円	50万円

※ ワンタイムパスワードをご利用のお客さまにつきましては従来通り1億円までご利用いただけます。

ご不明な点がございましたら、以下のフリーダイヤルまでお問い合わせください。

【お問い合わせ先】

山梨中銀ダイレクトマーケティングセンター

ふれあいハローに

フリーダイヤル 0120-201862<照会>ド：3>

(受付時間) 月曜日～金曜日 9:00～17:00 (ただし、祝日・12/31～1/3は除きます)

【山梨中銀Bizダイレクトをご利用のお客さまに講じていただくセキュリティ対策】

必須対策	
①	ウイルス対策ソフトを導入していただき、そのパターンファイル(ウイルス定義ファイル)は常に最新の状態に更新してください。
②	メーカーのサポートが終了したOS、ウェブブラウザは使用しないでください。 また、OS、ウェブブラウザは、最新の更新プログラムを適用してください。
③	ID・パスワードの管理を徹底してください(パソコン上にID・パスワードを保存しない、パスワードを定期的(最長でも90日毎)に変更するなど)。
推奨対策	
①	フィッシング詐欺対策ソフトを導入してください(当行ではフィッシング対策ソフト「PhishWallプレミアム」を無償提供しています)。
②	不審なログイン履歴や、身に覚えがない取引履歴・予約取引、取引通知メールがないか、定期的(毎朝)に確認してください。
③	不審な(例えば、山梨中央銀行を装った)メールの開封や、不正なサイトへのアクセスは行わないでください。また、不審な事象があった場合は、山梨中銀Bizダイレクトの利用を直ちに中止し、お取引店または、ダイレクトマーケティングセンターへ連絡してください。
④	承認機能を利用してください(取引の担当者と承認者を分ける)。また、担当者と承認者は別々の端末を使用してください。
⑤	[メール通知パスワードをご利用のお客さま] 山梨中銀Bizダイレクトを操作する端末と、メールを受信する端末を分けてください。
⑥	山梨中銀Bizダイレクトに登録するメールアドレスに、Yahooメール等のフリーメールは設定しないでください。
⑦	[電子証明書をご利用のお客さま] 電子証明書の管理を徹底してください(電子証明書を格納したままパソコンを破棄または譲渡しない、電子証明書が不正に削除されていた場合は不用意に再発行を行わないなど)。
⑧	振込・振替限度額を可能な限り低く設定してください。
⑨	各種パスワードを入力する際は、ソフトウェアキーボードを利用してください。
⑩	その他のソフトウェア(アクロバットやフラッシュプレイヤー等々)についても、最新の更新プログラムを適用してください。
⑪	山梨中銀Bizダイレクトを使用するパソコンは、インターネットバンキング専用のパソコンを用意してください。
⑫	パソコン(山梨中銀Bizダイレクト)を使用しない時間帯は、LANケーブルを抜くなど、インターネットに接続できない状態にしてください。