

## 法人 I B (WEB-FB) セキュリティ対策のお願いについて

当金庫の法人向けインターネットバンキング [WEB-FB] (以下「法人IB」という) サービスをご利用いただきまして厚く御礼申し上げます。

さて、マスコミ等で報道されていますようにコンピュータウイルス感染等により「インターネットバンキングで不正送金される」という被害が銀行を中心に発生しているため、不正送金被害対策としてお客さまによる適正なセキュリティ対策や取組みをお願いしているところです。

また、当金庫では、お客さまにご安心して法人IBサービスをご利用いただくため、不正送金被害に遭われた場合は、当金庫の規定等に基づき上限 1,000 万円まで補償する取組みを行っていますが、お客さまのセキュリティ対策度合などによっては、補償金額を減額または補償しない場合がありますので、下記の対策・取組みを適正に行っていただきますようお願いいたします。

### 1. 被害補償の要件について

被害に遭われた場合、下記の補償要件を満たしていることが条件になります。

- お客さまが不正利用に気づかれてから直ちに当金庫へ通知が行われていること。  
※不正取引発生日の翌日から 30 日を超えると補償対象外になります。
- お客さまが当金庫の調査に対し書面による十分な説明・提出を行い、これらの内容に不自然な点が認められないこと。
- 捜査機関(警察)に被害届を提出し、捜査に協力していること。
- 当金庫に被害状況を説明のうえ当金庫の調査に協力し、不正送金等が行われた時点において**適正にセキュリティ対策を講じていたこと**を当金庫に示していること。

※被害補償の詳細は、別紙「法人IB(WEB-FB)の不正送金に対する被害補償について」をご覧ください。

### 2. セキュリティ対策と被害に遭わないための取組みについて

被害補償要件の一つである「適正なセキュリティ対策を講じている」ことが、不正送金等の被害防止になりますので、日頃から適正に対策を講じていただきますようお願いいたします。

また、下記の取組みは、法人IBをご利用の担当者だけではなく、法人IBを利用するパソコンを操作する担当者につきましても下記対応を周知していただきますようお願いいたします。

#### ID・パスワード等の盗取対策として

ID・パスワード等の適正な管理は、かなり高い確率で不正アクセスを防御できるといわれています。

- ① ID・パスワード等は、第三者が容易に認知できるような形でメモ等を書き記すことなく、また、これら重要情報記載の書面等は第三者に知られないよう適正に保管してください。  
☞ ID・パスワード等は、担当者以外の方に知られないように保管してください。  
また、担当者の異動があった場合は、速やかにパスワード等を変更してください。
- ② 長期間同じログインパスワードおよび都度振込送信確認用パスワード(10桁)を使用することなく、定期的に変更してください。この際は、推測されやすいパスワード(生年月日、電話番号、車のナンバー等)を設定しないでください。

- ☞ 都度振込送信確認用パスワード(10桁)については、定期的に変更(短期間が望ましい)することにより、万が一、当該パスワードが盗取されても変更後は不正送金被害の防止になります。
- ③ 都度振込の振込限度額は可能な限り低い金額に設定変更してください。振込限度額の変更は、当金庫にお届けの限度額内であればお客さま自身で自由に変更できます。
  - ☞ 例えば、都度振込を利用しない間は限度額を千円に設定し、都度振込利用時に限度額を引き上げる取扱いも不正手段によっては有効ですが、当金庫にお届けの限度額を可能な限り低い金額で設定するとさらに有効的です。
  - ☞ 当金庫にお届けの限度額変更を要望される場合は、当金庫窓口にて所定の手続きをお願いします。
- ④ ID・パスワード等が盗取された場合または盗取された疑いがある場合は、すみやかに当金庫のIB担当まで連絡ください。
  - ☞ 不正取引を発見または不正取引の疑いがある場合についても、直ちに当金庫のIB担当に連絡ください。30日以内に連絡がないと被害補償が受けられなくなります。

#### ウイルスに感染しないために

- ① ウイルス対策ソフトを必ず導入してください。
  - また、使用期限が過ぎていないことを確認してください。
  - ウイルス対策ソフトの選定にあたっては、フリーウェアのウイルス対策ソフトを避けていただき、信頼できる市販のウイルス対策ソフトの導入を推奨します。
  - ☞ 不明な場合は、パソコンの購入業者にご相談ください。
- ② ウイルス対策ソフトのパターンファイルは常に最新の状態に更新し、定期的にウイルス検査を実施してください。
  - ウイルス対策ソフトの自動更新機能および自動検査機能を利用すると、これらの失念防止になります。
  - ☞ 不明な場合は、ウイルス対策ソフトの問合せ先にご確認ください。
- ③ 身に覚えのない電子メールは開かないようにしてください。
  - ☞ 万が一、開いた場合は、ウイルス対策ソフトでウイルス検査を実施してください。
- ④ 電子メールの添付ファイルまたはホームページ等からダウンロードしたファイルについて、使用する前にウイルス対策ソフトでウイルス検査を実施してください。
- ⑤ 法人IBを利用するパソコンで、不審なホームページへのアクセスやフリーソフト等のインストールなどはなるべく避けてください。
  - ☞ この場合は、速やかにウイルス対策ソフトでウイルス検査を実施してください。
- ⑥ ブラウザおよびOSは、常に最新の状態に更新してください。また、サポート終了のOS、ブラウザ、ウイルス対策ソフトなどは使用しないでください。
  - Windows Update を自動更新設定にするとOS等は最新状態に自動更新されます。
  - ☞ Window XPはマイクロソフト社のサポートを終了しています。
  - ☞ 当金庫インターネットバンキング推奨OSをご利用ください。(当金庫ホームページに掲載)

## 不正取引手口の主な特徴

被害のあった金融機関の発表や各種報道などから、最近の犯罪手口は主に次の3通りが多くみられています。

### ① 偽の画面を表示しパスワードを盗取する手口(MITB攻撃)

振込用の確認パスワードを入力する偽画面を表示することにより利用者にパスワードを入力させ盗取し、その盗取したパスワードを用いて不正送金を行う手口です。

《MITB(Man In The Browser)攻撃とわれている手口》

ウイルスがブラウザを乗っ取り、自由に画面表示を変えたり、入力データの盗聴、送信データの改ざんなどを行う攻撃。

### ② 電子証明書が入ったPCを遠隔操作により不正送金する手口

電子証明書方式では、電子証明書が入ったパソコン以外ではIB取引ができませんが、犯人は電子証明書が入ったパソコン自体を遠隔操作して不正送金を行う手口です。

### ③ 電子証明書をエクスポートして盗取する手口

ブラウザの電子証明書のエクスポート機能(バックアップ機能)を用いて電子証明書を盗取し、犯罪者のパソコン等に電子証明書をインポート(リストア)することにより不正送金を行う手口です。

※当金庫の法人IBでは、電子証明書のエクスポート(バックアップ)をできない設定に一律変更しています。

※ブラウザ：インターネットサイトを閲覧するソフトをいう。

代表的なブラウザは、IE(インターネット・エクスプローラ)。

## 偽の画面ってどんな画面？

一例ですが、下記のようにログイン後に不正な偽の画面を表示させ、都度振込送信確認用パスワード(10桁)などを入力させようとする事象が確認されておりますのでご注意ください。

当金庫の法人IBサービスでは、振込確認時の画面または都度振込送信確認用パスワード(10桁)の変更画面以外から入力を求めることは絶対にありませんので、下図のような画面が表示されても絶対に入力することなく直ちに当金庫・IB担当までご連絡ください。

《不正画面のメッセージの例》

例1. 平成25年12月に紹介された不正画面のメッセージ例

あなたのコンピュータをシステムが認識できませんでした。

インターネット・サービスプロバイダーが行った最近の変更、またはあなたが行ったソフトウェアの更新による可能性があります。引き続きバンキングサービスを利用するには、表からコードを入力してください。

	1	2	3	4	5	6	7	8	9	10	<input type="text"/>
確認番号				●			●	●	●		

ログイン

## 例2. 平成27年2月に紹介された不正画面のメッセージ例

あなたのコンピュータをシステムが認識できませんでした。

インターネット・サービスプロバイダーが行った最近の変更、  
または、ソフトウェアの更新による可能性があります。  
引き続きバンキングサービスを利用するには、表からコードを入力してください。

都度振込送信確認用パスワード1	都度振込送信確認用パスワードの左から1桁目を入力してください。	<input type="text"/>
都度振込送信確認用パスワード2	都度振込送信確認用パスワードの左から6桁目を入力してください。	<input type="text"/>
都度振込送信確認用パスワード3	都度振込送信確認用パスワードの左から7桁目を入力してください。	<input type="text"/>
都度振込送信確認用パスワード4	都度振込送信確認用パスワードの左から9桁目を入力してください。	<input type="text"/>

ログイン

### 当金庫の対応とお客さまへのお願い

- ① 金融業界の被害状況・取組みおよび当金庫の新たな取組みなどについて、必要に応じて、当金庫ホームページ、電子メール、郵送等によりお客さまに適正な情報(注意喚起)をお届けします。

また、不正送金被害等の発生状況により、お客さまあてに緊急連絡をさせていただく場合がありますので、連絡先に変更がありましたら直ちに設定変更または当金庫所定の手続きをお願いします。

- ☞ 当金庫にお届けの電子メールアドレスを変更された場合は、法人IB画面から新しいメールアドレスに変更してください。
- ☞ 口座名義・住所・電話番号などの当金庫にお届けいただいている事項が変更となる場合は、当金庫の取引店窓口にて所定の手続きを行ってください。

- ② セキュリティ対策として、電子証明書(有料)のエクスポート(バックアップ)は行えない設定に一律変更してあります。

- ☞ パソコンを機器更改した場合などは、お客さまが電子証明書の再発行を行ってください。
- ☞ セキュリティ対策強化として、電子証明書(有料)の導入をお薦めします。導入されるお客さまは、当金庫の取引店窓口にお申し出ください。

不正送金等の被害に遭わないように適正な取組みをお願いします。  
万が一、被害に遭った場合またはパスワード等を盗取された疑いのある場合は、直ちに当金庫のIB担当にご連絡ください。

《 連絡先 (IB担当) 》

柏崎信用金庫 事務部 IB担当  
電話: 0257-24-3321