

法人向けインターネットバンキングサービスに係る 預金等の不正な払戻し被害の補償対応について

最近のインターネットバンキングに係る預金等の不正な払戻しの手口は、コンピュータウイルスを利用したID・パスワードの搾取やパーソナルコンピュータ（以下、「PC」といいます。）の遠隔操作に見られるように、極めて高度化・巧妙化しています。

このような状況を踏まえ、当金庫では法人向けインターネットバンキングサービス（以下、「法人IB」といいます。）を安心してご利用いただくため、法人IBに係る預金等の不正な払戻し被害につきまして、当金庫所定の補償限度額の範囲内で補償を行うことといたしましたのでお知らせします。

本取組みは、平成26年7月17日付全国銀行協会の申し合わせ（法人向けインターネット・バンキングにおける預金等の不正払戻しに関する補償の考え方）を踏まえ対応するものです。

■ 補償の概要

1. 対象となるお客さま

当金庫のインターネットバンキング（だいしんWEB-FB、だいしんWEBバンキング）をご利用頂いている法人のお客さま

2. 被害補償の限度額

1口座あたり、原則、年間1,000万円を上限として被害額の補償を検討いたします。

なお、お客さまが電子証明書方式、ワンタイムパスワードやウイルス対策ソフトをご利用されていない場合など、補償の対象とならない場合がございます。

3. 被害補償の開始時期

平成27年3月2日（月）

4. 被害補償の適用条件等

搾取されたパスワード等を用いて行われた本サービスによる不正な払戻し（以下、「当該払戻し」といいます。）について、『ご利用をいただくうえで“必ず実施”していただきたいセキュリティ対策』の導入を前提に、次の各号に該当する場合、お客さまは当金庫に対して、補償限度額1,000万円の範囲内で当該取引に係る払戻しの損害（手数料・利息を含み、お客さまが不正払戻しを行ったものから受けた損害賠償金または不当利得返還金の額を除きます。）の補償を請求することができるものとします。

- (1) 不正使用に気づいてからすみやかに、当金庫への通知が行われていること
- (2) 当金庫の調査に対し、お客さまより十分な説明が行われていること
- (3) 当金庫に対し、警察署に被害届を提出していること、その他盗難にあったことが推測される事実を確認できるものを示していること

ただし、当該払戻しが行われたことについて、当金庫が善意無過失であること、およびお客さまに過失または重過失があることを当金庫が証明した場合には、当金庫は補償対象額の一部または全部を補償いたしかねる場合がございます。

【補償いたしかねる場合】（主なもの）

- ① 『ご利用をいただくうえで“必ず実施”していただきたいセキュリティ対策』を実施していなかった場合
- ② 不正払戻しの発生した翌日から 30 日以内に当金庫へ事故のお届けをいただけなかった場合
- ③ お客さまが日本国外にお住まい、または日本国外でご利用される場合
- ④ お客さまの社内、ご家族、または使用人自らの行為、もしくは加担した盗用によって生じた損害
- ⑤ 戦争、地震などによる著しい秩序の混乱に乗じてなされた不正使用によって生じた損害の場合

【補償を減額する場合】（主なもの）

- ① 本人確認情報であるログインID、各種パスワード、暗証番号等が適切に管理されていない場合
- ② 当金庫が推奨するOS（PC基本ソフト）、ウェブブラウザ（インターネット閲覧ソフト）以外で本サービスを使用している場合

◆ ご利用いただくうえで“必ず実施”していただきたいセキュリティ対策

- “無償提供”のセキュリティ対策ソフト「PhishWall プレミアム」をインストールしたPCで、同対策ソフトを利用してサービスを利用する。
- 「だいしんWEB-FB」をご利用のお客さまは、本人認証方法を「電子証明書方式」としてサービスを利用する。
- 「だいしんWEBバンキング」をご利用のお客さまは、本人認証方法を「ワンタイムパスワード」としてサービスを利用する。
- インターネットバンキングに使用するPCに関して、OSやウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新して利用する。また、製造・開発元のサポート期限が終了しているものは使用しない。
- インターネットバンキングに使用するPCに関して、お客さま自身でPCにウイルスソフトを導入するとともに、常に最新の状態に更新したうえで利用する。
- インターネットバンキングに係るパスワードを定期的に更新する。

◆ ご利用いただくうえで“推奨”するセキュリティ対策

- PCの利用目的として、インターネット接続時の利用はインターネットバンキングに限定して利用する。
- PCや無線LANのルータ等について、未利用時は可能な限り電源を切断する。
- 取引の申請者と承認者とで異なるPCを利用する。
- お振込の限度額を必要な範囲内でできるだけ低く設定する。
- 不審なログイン履歴や身に覚えがない取引履歴、取引通知メールがないかを定期的に確認する。

● 補償制度についての注意事項

補償制度をご利用いただくために、特別な申込は必要ありませんが、当金庫がセキュリティ対策として導入している「電子証明書」、「ワンタイムパスワード」および「ウイルス対策ソフト」のご利用等が必要となりますので、ぜひこの機会にご利用を検討ください。

○ 電子証明書（だいしんWEB-FBをご利用のお客さまが対象）

PCに「電子証明書」をダウンロードすることで、「電子証明書」がダウンロードされていないPCからは「だいしんWEB-FB」がご利用できなくなるサービスです。

利用できるPCを限定することで、仮に第三者に不正にパスワードを搾取されても、第三者が所有するPCには「電子証明書」がダウンロードされていないため、不正ログインを防止できます。

○ ワンタイムパスワード（だいしんWEBバンキングをご利用のお客さまが対象）

ワンタイムパスワードとは、ソフトウェアトークン（ワンタイムパスワードの生成・表示端末）を利用して、30秒毎に作成される使い捨てのパスワードにより、高いセキュリティを実現できるサービスです。

ワンタイムパスワードは、WEBバンキングサービスのログイン時に、従来の「契約者ID」と「ログインパスワード」の認証に加えて、ワンタイムパスワードの認証が追加されます。トークンに表示されているワンタイムパスワードを入力することでインターネットバンキングにログインできます。

ワンタイムパスワードは、1回限りの使い捨てのパスワードのため、万が一ウイルス等でパスワードが盗まれてしまった場合でも、不正利用を防ぐことができ、より安全にインターネットバンキングをご利用して頂くことができます。

なお、お客さまのスマートフォンや携帯電話をソフトウェアトークンとしてご利用いただくため、特別な機器をご用意いただく必要はありません。

○ ウイルス対策ソフト

当金庫では、ホームページからダウンロード可能なウイルス対策ソフト「PhishWallプレミアム」を無償で提供しております。

「PhishWallプレミアム」は、「だいしんWEB-FB」および「だいしんWEBバンキング」のご利用中に自動的に起動し、ウイルスの検知や無効化を行う効果があります。

本件に関するお問い合わせ先

大垣信用金庫 事務管理部

電話（代表）： 0584-75-6116

受付時間： 月曜日～金曜日（金融機関休業日を除く）

AM9:00～PM5:00