平成２７年１月
空知商工信用組合

法人向けインターネットバンキング（空知しんくみビジネスバンキング）預金の不正な払戻しに対する補償について

法人向けインターネットバンキング(空知しんくみビジネスバンキング)をご利用いただき、誠にありがとうございます。
ご利用にあたって、当組合の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な払戻しによる被害に対する補償制度は下記のとおりです。

記

■補償制度について

１．補償制度の概要

本補償制度は、空知しんくみビジネスバンキングご利用中のお客さまが第三者による不正アクセスを受け、預金等の不正な払戻しが発生した場合に、当組合がお客さまの被害を補償させていただく制度です。

２．補償金額

１口座あたり、年額２，０００万円を上限として被害額を補償いたします。

３．補償に関する注意事項

当組合が指定する所定のセキュリティ対策を実施されていない場合など、補償の対象外、もしくは補償を減額するケースがございます。

１ ≪補償の対象とならない又は補償の減額となる主なケース≫
２ ◆ご利用いただくうえで"必ず実施"いただくセキュリティ対策◆
３ ◆お客さまに講じていただくセキュリティ対策◆
４ 不正アクセス等によるインターネットバンキングでの被害について

をご確認のうえセキュリティ対策を実施してください。

◆補償制度の仕組み

空知しんくみビジネスバンキングにおいて、預金等の不正な払戻しに遭われた場合、１口座あたり、年額２，０００万円を上限に補償を実施するものです。
なお、具体的な補償の内容につきましては、お客さまのご利用状況やセキュリティ対策の導入状況および警察当局による捜査結果等を踏まえ、当組合が検討・判定した結果に基づきます。

１.≪補償の対象とならない又は補償の減額となる主なケース≫

①次ページに記載した、空知しんくみビジネスバンキング『ご利用いただくうえで“必ず実施”いただくセキュリティ対策』を実施していなかった場合

②身に覚えのない残高変動や資金の不正取引が発生した日の翌日から３０日以内に当組合へ被害のお届けをいただけなかった場合

③警察に被害届を提出しなかった場合

④不正取引が発生した際に、金融機関による調査および警察による捜査へご協力いただけなかった場合

⑤正当な理由なく、他人にログインＩＤ・ログインパスワード等を回答してしまった場合

⑥パソコンや携帯電話等が盗難に遭った場合において、ログインＩＤ・パスワード・暗証番号等をパソコンや携帯電話等に保存していた場合

⑦当組合が注意喚起しているにも関わらず、注意喚起された方法で、メール型のフィッシングに騙される等、不用意にログインＩＤ・パスワード・暗証番号等を入力してしまった場合

⑧お客さまの会社関係者、ご家族または使用人自らの行為、加担した盗用によって生じた損害の場合

⑨他人に強要されたインターネットバンキングの不正使用の場合

⑩電子メールアドレス、ご住所、お名前等の変更に係る当組合所定の手続が行われていない場合

⑪お客さまが日本国外にお住まい、または日本国外で利用されている場合

⑫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

⑬お客さまの故意、または重大な過失によって生じた損害の場合

２.◆ご利用いただくうえで"必ず実施"いただくセキュリティ対策◆

〇“無償提供”の不正送金対策ソフト「PhishWall プレミアム」をインストールしたパソコンで、同対策ソフトを利用してサービスを利用する。

〇インターネットバンキングに使用するパソコンに関し、基本ソフト（ＯＳ例：Windows）やウェブブラウザ（例：Internet Explorer）等、インストールされている各種ソフトウエアを最新の状態に更新する。

〇パソコンにインストールされている各種ソフトウエアで、メーカーのサポート期限が経過した基本ソフトやウェブブラウザ等は使用しない。

〇お客さまご自身でパソコンにウイルス対策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。

〇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。

〇電子証明書を導入し、当組合が指定した正規の手順以外での電子証明書の利用はしない。

3.◆お客さまに講じていただくセキュリティ対策◆

平素より空知商工信用組合をご愛顧賜り誠にありがとうございます。
インターネットバンキングをより安全にご利用いただくため、以下の対策をお願いします。

＜ウイルスがお客さまのパソコンへ侵入することを防ぐための注意点＞

	実施する内容	実施することによる効果
①	基本ソフト OS（（例）Windows）ブラウザ（（例）Internet Explorer）等は、常に最新の状態に更新してください。	更新情報にはセキュリティ対策に必要な修正プログラム等が含まれています。
②	サポート期限が経過している基本ソフト等の利用はお控えください。	サポートが終了した基本ソフト等のご利用を続けるとウイルスに感染しやすい環境になります。
③	ウイルス対策ソフトを導入し、常に最新の状態に更新してください。	日々新しく誕生するコンピュータウイルスに対応するパターンファイルが更新されます。
④	不審なメールの開封および不審なサイトの閲覧は控えてください。	開封するだけで感染するウイルスが存在している可能性があります。
⑤	必要性がないダウンロード、USB 等の外部記録媒体の使用はしないでください。	ダウンロードするファイルやデータにウイルスが存在している可能性があります。
⑥	当組合よりご案内する不正送金対策ソフト“PhishWall プレミアム”をインストールしてください。	市販のウイルス対策ソフトと併用することで不正送金を防止できる可能性が高まります。
⑦	インターネットバンキング専用のパソコンを用意していただき、可能な限り他の事で使用しないでください。	ウイルス感染防止に繋がります。
⑧	長時間操作を中断する場合はパソコンや無線 LAN のルータ等の電源を切ってください。	遠隔操作等の不正ログイン防止に繋がります。

＜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の対策＞

	実施する内容	実施することによる効果
①	パスワード等を定期的に変更してください。（推奨：1ヶ月に一度変更） パスワード入力時はソフトウェアキーボード推奨。	定期的に変更することで漏洩したパスワードが利用できなくなります。
②	振込などの限度額を必要な範囲内で出来る限り低く設定してください。	不正送金被害を最小限に抑えられます。
③	取引時の通知メールは直にご確認してください。	不正送金被害の早期発見に役立ちます。
④	不審な前回ログイン履歴がないかログイン時に確認してください。	不正履歴が確認された場合、直ちに ID・パスワード等を変更し不正なログイン防止に繋がります。
⑤	ID・パスワード等は、利用者以外に教えないでください。	パスワード漏洩リスクを低減軽減できます。
⑥	通常とは異なる画面が表示された場合、直ちに操作を中止し、当組合までご連絡ください。	不正送金被害の防止に繋がります。
⑦	インターネットバンキングをご利用になる際には、利用前にセキュリティソフトでウイルスチェックを行い、ウイルス感染がないことをご確認のうえでのご利用をお願いします。	ウイルス感染の早期発見に役立ちます。
⑧	振込の申請者と承認者とで異なるパソコンをご利用ください。	申請者でデータ改ざんされた場合でも承認者で不正送金を防止できます。
⑨	ログインは電子証明書方式をご利用ください。	電子証明書方式は使用パソコンを限定でき不正なログイン防止に繋がります。
⑩	電子証明書方式は、当組合が指定した正規の手順でご利用ください。	正規の手順以外で利用されると電子証明情報が漏洩されます。

※上記対策を講じていても完璧なセキュリティ対策が保証されたわけではありませんが安全性は向上します。

４.不正アクセス等によるインターネットバンキングでの被害について

現在、お客さまのパソコンから、インターネットバンキングの ID やパスワード、暗証番号等をウエブサイトやダイレクトメール等、様々な方法により不正に取得し、お客さまに気付かれずにお客さまの口座から不正に現金を引き出す被害が、全国の金融機関で発生しています。
最近、多発している主な不正送金の手口は、次のようなものです。

＜コンピュータウイルスを利用したもの＞

〇送付したメールやお客さまが閲覧したサイトから、お客さまのパソコンをウイルスに感染させ、ウイルスの働きにより、お客さまが気づかないうちにお客さまの預金口座から不正送金が行われる。

不正なコンピュータウイルスには、主に、以下のようなものがあります。

【不正送金ウイルス】

不正送金ウイルスとは、パソコンに感染したウイルスが、インターネットバンキングの利用等に伴い働き、お客さまの操作とは関係のない先へ、不正な送金を行うウイルスです。

【スパイウエア】

スパイウエアとは、感染したウイルスが勝手に、お客さまのパソコンに記録されている ID やパスワードなどの重要情報を、第三者へ転送してしまうウイルスです。

＜フィッシングによるもの＞

〇銀行等の企業であるかのように装った電子メールを不特定多数のお客さまに送付し、偽のホームページへ誘導し、お客さまに入力させて取得した ID やパスワード等を利用して、不正にお客さまの預金口座から送金を行う。

〇正規のホームページの閲覧中やインターネットバンキングへのログイン後に、不正なポップアップ画面が表示され、そこに入力させることで取得した ID やパスワード等を利用して、不正にお客さまの預金口座から送金を行う。

※当組合ではポップアップ画面によるお客さまの情報入力画面はありません。

＜その他の手口＞

〇当該金融機関を偽装した CD－ROM を郵送し、その CD―ROM から「スパイウエア」等のウイルスをインストールさせ、その「スパイウエア」により取得したお客さまの ID、パスワード等を利用し、不正にお客さまの預金口座から送金を行う。