お客様各位

株式会社　北海道銀行

道銀ビジネスＷＥＢサービスをご利用のお客様へ大切なお知らせ

拝啓

平素は北海道銀行をご利用いただき誠にありがとうございます。

また、法人インターネットバンキング「道銀ビジネス WEB サービス」をご利用いただき重ねてお礼を申し上げます。

さて、新聞等でも報道されておりますとおり、悪意の第三者によるインターネットバンキングの不正な払出しが多発しております。お客様の「ログイン ID」・「ログインパスワード」等を盗み取り、不正送金を行って現金を搾取する犯罪が後を絶ちません。

弊行におきましては、不正送金等の被害は今のところございませんが、不正ログインされたと思われる事象が報告されております。

弊行では、「電子証明書の導入」、「ソフトウェアキーボードの導入」、「都度指定の振込・振替の当日扱い停止」、「フィッシング対策ソリューション「PHISHCUT（フィッシュカット）」のご提供」、「EV SSL 証明書」の導入によりお客様の大切なご預金をお守りしておりますが、不正アクセスによる被害を防止するには、お客様におかれましてもセキュリティ対策が不可欠です。

お客様におかれましても講じていただきたいセキュリティ対策を以下に記載いたしますので、ご一読いただき、今一度ご確認いただきますようお願いいたします。

【お客様に行っていただきたいセキュリティ対策】

１．弊行が推奨しているセキュリティ対策（フィッシング対策ソリューション「PHISHCUT」の導入、電子証明書方式のご利用）の実施。

２．インターネットバンキングに使用するパソコンの基本ソフト（OS）やインターネット閲覧ソフト（ウェブブラウザ）等を最新の状態に更新する。

３．インターネットバンキングに使用するパソコンにインストールされている各種ソフトウェアで、Windows XP のようにメーカーのサポート期限が経過した基本ソフト（OS）やインターネット閲覧ソフト（ウェブブラウザ）を使用しない。

４．インターネットバンキングに使用するパソコンには「必ず」セキュリティソフトを導入する。また、セキュリティソフトは「常に最新の状態」に更新する。

５．ビジネス WEB サービスの「ログインパスワード」「確認用パスワード」を定期的に変更する。決してファイル等に保存しない。

これらの対策を施していないパソコンでは、お客様の「ログイン ID」・「ログインパスワード」等が盗取される恐れがありますので、「都度指定振込（予約扱）」のご使用は避け、「事前登録方式」でのご使用をお勧めいたします（別途お申込み・登録手続が必要です）。

また、道銀ビジネスWEBサービスを安心してご利用いただくために、以下のセキュリティ対策をお勧めいたします。

【お客様にお勧めするセキュリティ対策】

１．インターネットバンキングに使用するパソコンは、常時のインターネット接続を避ける。

２．インターネットバンキングに使用するパソコンや無線LANのルータ等は、未使用時は可能な限り電源を切断する。

３．データ伝送サービス（総合振込・給与振込）においては、取引データの作成者と承認者はできるだけ異なるパソコンを利用する。

４．振込・振替限度額は必要な範囲内に設定する。

５．不審なログイン履歴や身に覚えのない取引履歴、通知メールがないかを定期的に確認する。

【ご参考】

以下の項目にあてはまる場合は、パソコンがコンピューターウィルスに感染した可能性がありますのでご注意願います。

・電子証明書が消失した
・急にパソコンの動きが遅くなった
・パソコンの利用中にメモリ利用率が異様に高くなる
・自動的にコマンドプロンプトが表示される

なお、弊行では、新たなセキュリティ対策を検討しておりますので、詳細が決定次第あらためてご案内いたします。

また、最近、「電子証明書が突然消失した」等異常を感じられましたら、お取引店または弊行ダイレクトバンキングセンターまでご一報いただきますようお願いいたします。

敬具

【お問い合わせ先】
北海道銀行ダイレクトバンキングセンター
0120-44-5589（音声ガイダンス「1」を選択）
携帯電話からは、011-818-0393
（受付時間　銀行営業日：9:00～17：00）

（平成２６年９月）