インターネットバンキングご利用に関する注意点

2014 年 9 月

English Message Follows:

法人のお客さま向けインターネットバンキングでの不正送金被害が一部の金融機関で発生しております。

ご利用のパソコンにウイルスやスパイウェア等に感染させ、遠隔操作をおこない不正送金を行うという手口が報告されています。弊行では HSBC*net* でさまざまなセキュリティ対策を行っておりますが、パソコンのウイルス、スパイウェア等の感染や不正送金の被害発生等を防ぎ、サービスをより安全にご利用いただくため、以下の点にご注意いただきますようお願いいたします。

1. お客様に必ず実施していただくセキュリティ対策

- HSBCnet でご提供している以下のセキュリティ関連機能をご利用ください。ご利用方法に関して、ご不明な点につきましては弊行担当者までお問い合わせください。
  - ① セキュリティデバイスおよびスマートカードの利用
  - ② 二重および三重送金承認機能の利用
  - ③ 承認限度額の設定
  - ④ カスタマーアラートの設定

- OS やブラウザ、ソフトウエア等は、必ず最新版に更新してご利用ください。また、更新後は、古いバージョンのソフトがパソコン上に残っている場合はアンインストールしてください。

- OS やブラウザ、ソフトウエア等で、メーカーのサポート期限が経過したものは利用を中止してください。

- セキュリティ対策ソフトを導入いただき、常に最新の状態に更新し、定期的にウイルスチェックと駆除を行ってください。

- セキュリティデバイスおよびスマートカードのパスワードは決して第三者に知らせないでください。また、第三者が指定するパスワード等は使用しないでください。生年月日、自宅や勤務先の住所・地番・電話番号、同一数字や連番等の推測されやすいパスワードの使用を避け、定期的に変更してください。

- スマートカードに関して、決められた手順に従ってご利用ください。

- 心当たりのない宛先からの電子メールに添付されているファイルの開封や URL のクリックは行わず、速やかに削除してください。また、不審な WEB サイトへアクセスしないでください。

- 前回のログイン時間をご確認いただくとともに、心当たりの無い取引がないか、取引履歴をこまめにご確認ください。

- 送金作成者と承認者は分けていただき、別々のパソコンで利用してください。

2. お客様に推奨されるセキュリティ対策

- HSBCnet でご提供している以下のセキュリティ関連機能を、可能な限りご利用ください。ご利用方法に関して、ご不明な点につきましては弊行担当者までお問い合わせください。
  - ① Webroot Secure Anywhere のダウンロード
  - ② IP アドレスの登録
  - ③ 制限付きテンプレート（振込先を限定する機能）の利用

- 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 のルーター等について、未利用時は可能な限り電源を切断してください。

- インターネットバンキングに使用するパソコンの利用目的を限定することをお勧めします。また、使用者を限定し、不特定多数の人が操作できないパソコンでご利用ください。

- 取引限度額は必要な範囲でできるだけ低く設定することをお勧めします。

お客様が上記のセキュリティ対策を実施されずに不正送金被害にあわれた場合には、弊行では被害補償の対象外とさせていただくことがあります。

万一、不審な取引などをご確認された場合は、弊行へご連絡いただくとともに、最寄りの警察署にもご相談いただきますようお願いいたします。

本件につきましてご質問等ございましたら、以下の連絡先までお問い合わせ下さい。

香港上海銀行東京支店　グローバルキャッシュマネージメント部

電話: 03-5203- 3247

メール: jcsc@hsbc.co.jp

Important reminder using the Internet Banking

September 2014

There have been many recent reports of fraud involving banking accounts, transactions, and activities from some financial institutions in Japan. Malware and Spyware pose a serious threat as they can be used to steal data from your PC and this information can be used to conduct fraudulent transactions.

While various security measures have been implemented by HSBC, in order to better ensure the safe and secure use of our services, please note the following guidelines:

3. Required security measures for corporate customers

- Properly implement security measures provided by HSBC*net*. If you have any questions, please contact your local HSBC*net* Support Centre or HSBC representative.
  - ① Use Security device or Smart card.
  - ② Apply dual authorization or triple authorization for payment creation.
  - ③ Set daily transaction limits.
  - ④ Set customer alerts.

- Keep all software applications such as your operating system or internet browser, up-to-date. Uninstall old versions of software from your computer.

- Stop using software applications for which the vendor no longer provides support.

- You may already be using anti-virus software but to ensure it is effective, the software should be updated with the latest virus definition files. Perform virus checks on a regular basis and ensure computer viruses are removed from your system, if applicable.

- Your HSBC*net* password, together with other internet banking credentials, permits access to your bank account. When creating passwords, remember the following:
  - ✓ Keep passwords to yourself: No one at HSBC will ever ask you for your internet banking password.
  - ✓ Make passwords hard to guess.
  - ✓ Make variations: Try to use different passwords for different services.
  - ✓ Change passwords regularly.
  - ✓ Never write passwords down.

- Follow and adhere to HSBC's guidelines when using Smart Card devices.

- Never click embedded hyperlinks nor open attached files in emails from untrustworthy sources, and do not access suspicious websites.

- Review transaction records regularly and check your last HSBC*net* login time and ensure it is accurate.

- Entitle payment creators and authorisers to different individuals. When authorising a transaction, use a different computer from the one that the instruction was created on.

4. Recommended security measures for corporate customers

- Implement security measures which are provided by HSBC*net*. If you have any questions, please contact your local HSBC*net* Support Centre or HSBC representative.
  - ① Download Webroot *SecureAnywhere* online protection software, available via HSBC*net*.
  - ② Raise the request to bank for IP address restriction.
  - ③ Use Restricted Templates for payment creation.

- When not in use, shut down your computer, Wi-Fi router etc. as much as possible.

- Payment creators and authorisers should use different computers.

- Set conservative payment, transfer and refund limits as much as possible.

Please be advised that in no event shall any damage caused by internet banking fraud attacks be compensated if you have not taken the proper security measures set forth above.

If you suspect an online fraud, immediately contact your HSBC representative and the police.

If you have any questions, please contact us at:

The Hongkong and Shanghai Banking Corporation Limited, Global Payment and Cash Management

Tel: 03-5203- 3247

E mail: jcsc@hsbc.co.jp