TOKYO STAR BANK
東京スター銀行

News Release

2005 年 3 月 23 日

東京スター銀行
日本企業初!!
フィッシング詐欺対策機能を持ったツールを導入
～自社ホームページの個人情報保護を強化し、お客さまに安全と安心を提供～

株式会社東京スター銀行（東京都港区：代表執行役 CEO　タッド・バッジ）は、2005 年 3 月 29 日より、日本で初めて、フィッシング詐欺対策機能を持った個人情報保護ツール「nProtect Netizen(エヌプロテクトネチズン)」を当行ホームページに導入いたします。東京スター銀行のホームページをご利用いただいておりますお客さまに対して、安全・安心をご提供できるツールであり、これにより、アクセス中の個人情報保護のさらなる強化を図ります。

この個人情報保護ツールは、お客さまが東京スター銀行のホームページにアクセスしている間、「コンピュータウィルスへの感染」や「スパイウェア、キーログハッキングによる個人情報の盗難」、「フィッシングによる被害」を防ぎます。お客さまは、東京スター銀行のホームページ上にあるこの個人情報保護ツールを起動するだけで、フィッシングやウイルス感染などによる被害を心配することなく、安心してホームページをご利用いただけます。特に、最近被害が拡大しているフィッシング詐欺に対しての有効な対策機能である「フィッシングブロック」機能を導入するのは、東京スター銀行が日本で初めてとなります。

この「フィッシングブロック」機能は、ツールを起動するだけで、お客さまがアクセスしようとしているサイトが、正規の東京スター銀行のサイトかどうか、簡単に判別することができます。もちろん、フィッシング詐欺は企業側の努力だけで防げるものではありません。この画期的なツールを無償提供することで、広くお客さまにご活用いただき、共闘してフィッシング詐欺に対策できることを目的としております。東京スター銀行はこれからも、お客さまに安全・安心をご提供すべく、努めてまいります。

■「フィッシングブロック」の特長

・フィッシングブロック【新機能】

URL を本物と見せかけ、大事な個人情報を横取りしようとするウェブサイトを「フィッシングサイト」と呼びます。フィッシング詐欺対策機能ツールが起動している間、これを起動させたウェブサイトとは関係のない URL を開こうとした際に、注意を促すメッセージダイアログを表示させます。このメッセージにて、お客様は上記サイトが正規のサイトかどうかを、簡単に判断することができます。

■「nProtect Netizen(エヌプロテクトネチズン)」の他の機能

・AntiWorm（アンチワーム）【世界最先端機能】

ネット接続のみで感染してしまうワームウィルスに対し、パソコンへの侵入前に行動を検知、感染からブロックします。

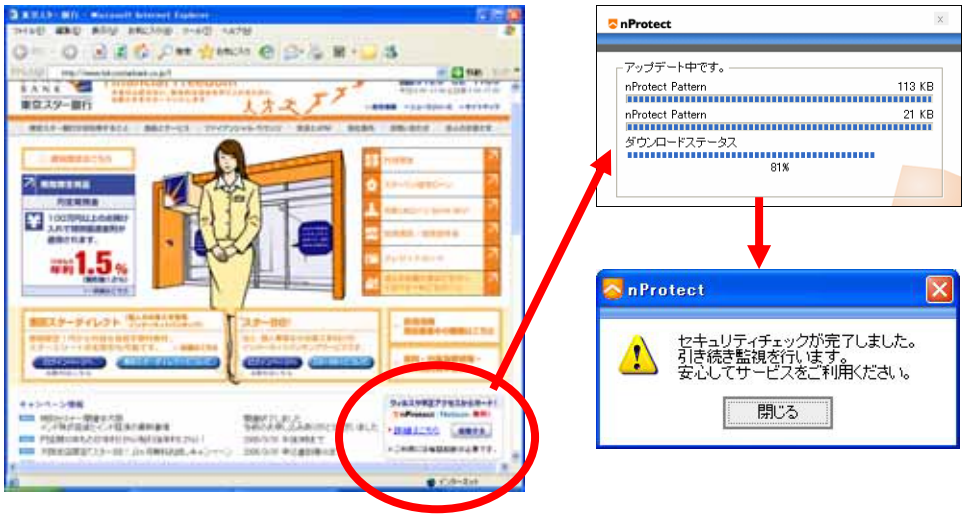
・KeyCrypt（キークリプト）【世界最先端機能】

キー入力した内容を暗号化（あらかじめ決められた文字に自動変換）し、ハッキング行為自体を無力化、情報の漏洩からガードします。

■使用方法

例：東京スター銀行のお客さまのもとに、東京スター銀行を装ったフィッシング詐欺のメールが届いたとします。メールに書かれている URL がフィッシングサイトかどうかを判断したい場合、以下のようにします。

1. 東京スター銀行のホームページ（http://www.tokyostarbank.co.jp）にアクセスし、「nProtect Netizen」を起動します。（メールに書かれている URL を直接クリックしないでください。）



2. 別のブラウザウィンドウを立ち上げ、メールに記載されている URL をクリックしてそのサイトを開きます。もしこのときに、『東京スター銀行とは関連のないホームページにアクセスしました。』というメッセージダイアログが表示されたら、そのサイトはフィッシングサイトである可能性があります。

なぜ、この様にフィッシング詐欺対策が可能になったかと言うと、フィッシング詐欺対策機能を持った個人情報保護ツール「nProtect Netizen」には、東京スター銀行に関連のあるIPアドレスが予め登録されています。もしフィッシングサイトをブラウザで開いた場合、ツール自らがこのフィッシングサイトのIPアドレスを調べ、予め登録されているIPアドレスの中にそのアドレスが見つからない場合はメッセージダイアログを表示させる仕組みとなっています。