2005 年 4 月
株式会社クレディセゾン

クレディセゾン　ホームページ
フィッシング詐欺にも対応した個人情報保護ツールを導入
～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～

株式会社クレディセゾン（東京都豊島区：代表取締役　林野　宏）は、2005 年 4 月 25 日より、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)」をホームページに導入いたします。「nProtect Netizen」は、クレディセゾンのホームページをご利用いただいるお客様に対して、安全・安心を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「nProtect Netizen」は、お客様がクレディセゾン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。お客様は、ホームページ上にあるこの「nProtect Netizen」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、安心してインターネットをご利用いただけます。

nProtect Netizen **の最大の特徴である「フィッシングブロック」機能は、ツールを起動するだけで、お客様がアクセスしようとしているサイトが、正規のクレディセゾンのサイトかどうか、簡単に判別することができます。この画期的なツールを無償提供することで、広くお客様にご活用いただき、安心してインターネットをご利用いただける環境を整えていくことを目的としています。**

「nProtect Netizen(エヌプロテクトネチズン)」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。

◇フィッシングブロック
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。
※フィッシング、スパイウェア、キーログハッキングなどの用語説明は別紙をご参照ください。

「nProtect Netizen(エヌプロテクトネチズン)」について

◇開発元：インカ・インターネット
（韓国企業）
◇日本国内代理店：ネットムーブ株式会社
（日商エレクトロニクス グループ企業、渋谷区渋谷 3-9-10-5F、代表取締役社長：澤田富仁）

クレディセゾンでは、顧客ニーズに敏感に対応し、独自性あふれるサービスを開発推進していくことで、常にお客様のライフスタイルをサポートする「サービス先端企業」となることを目指しています。今後もこれまで以上に顧客視点に立ったサービス構築に取り組み、さらにお客様に「安全」・「安心」をご提供すべく努めてまいります。

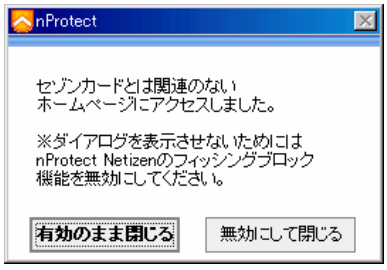
nProtect Netizen の起動の方法

クレディセゾンのホームページ（http://www.saisoncard.co.jp）にアクセスし、「nProtect Netizen 起動ボタン」をクリックして　起動します。
※パソコンを立ち上げる際には毎回この作業が必要となります。

※　別のブラウザを立ち上げる際にもセゾンカードのホームページブラウザを立ち上げていれば nProtect Netizen が起動し、お客様のパソコンを守り続けます。

「フィッシングブロック」の使い方

個人情報等の入力を求めるメールが届いた場合、別のブラウザウィンドウを立ち上げ、クレディセゾンホームページにアクセスし、nProtect Netizen を起動します。その後、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、『セゾンカード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となったのか

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、クレディセゾンに関連のある 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。

◇　この件に関するお問い合わせ先　◇
㈱クレディセゾン　広報室　佐藤・廣瀬
TEL（03）3982－0700　email ： prir@mail.saisoncard.co.jp
◇　サービスに関するお問い合わせ先　◇
TEL（03）3409－5231　email ： nprotect-sup@netmove.co.jp

（参考）用語説明

◇ スパイウェア

お使いのパソコンから情報を収集・送信するプログラムです。多くはソフトウェアやブラウザなどとともにインストールされ、利用の時点で「情報収集が行われる」ことが明らかにされています。しかし、中には通知せずに個人情報を送信する、悪質なプログラムも存在します。

◇ キーログハッキング

キーボードからの入力情報を不正に記録するプログラム（キーロガー）をパソコンに潜入させて、ID やパスワード、カード番号などを奪うハッキング行為です。キーロガーの潜入は、ウイルスどと同じくメールの添付ファイルとして侵入するケースや、利用するパソコンに第三者が事前仕掛けている場合などがあります。

◇ フィッシング詐欺

本物のサービスと見せかけたウェブサイト（フィッシングサイト）を使った詐欺の手法を「フィッシング詐欺」と呼びます。よくある手口としては以下の様なものがあります。

[1] フィッシングサイトの URL を記載し、あたかも○△銀行であるかのように装った広告メールを流布
[2] そのメールを本物の○△銀行からのものと思い、フィッシングサイトにアクセス
[3] フィッシングサイト内でユーザID、パスワード、カード番号などを入力
[4] ○△銀行とはまったく関係のない第三者に、それらの個人情報が流出